**相册簿管理系统的设计与实现**

指导老师：李懿

（浙江中医药大学医学技术学院，杭州，浙江 310053）

**摘 要**：近年来，人们对精神方面的需求越来越多，比如拍照去记录自己的生活和身边的事物。现代的拍照工具都是电子设备所以照片会以图像格式存储在设备中，然而，设备通常不能帮你去分类和管理照片，它们只会以时间顺序先后排列。在以前，人们可以买一本相册簿往里面摆放自己的照片甚至可以写上文字加以注释，现在，人们同样也需要，只不过我们将其变成了电脑版。该相册簿管理系统可供用户高度自定义编辑自己的相册簿和管理多本相册簿，为了保障用户个人信息的安全，我们将用户信息存储在服务器并进行加密处理。

**关键词**：电子相册，系统设计，java，数据库

**Design and implementation of album management system**

Director：Yi Li

（College of Medical Technology, Zhejiang Chinese Medical University, Hangzhou, China, 310053）

**Abstract**: In recent years, people have more and more spiritual needs, such as taking photos to record their lives and things around them. Modern photography tools are electronic devices, so photos will be stored in the device in image format. However, the device usually can't help you to classify and manage photos. They will only be arranged in chronological order. In the past, people could buy an album to put their own photos in it or even write words to annotate it. Now, people also need it, but we have turned it into a computer version. The album management system allows users to edit their own albums and manage multiple albums. In order to ensure the security of users' personal information, we store the user information on the server and encrypt it.

**Key Words**: Electronic album; system design; java;database

引 言

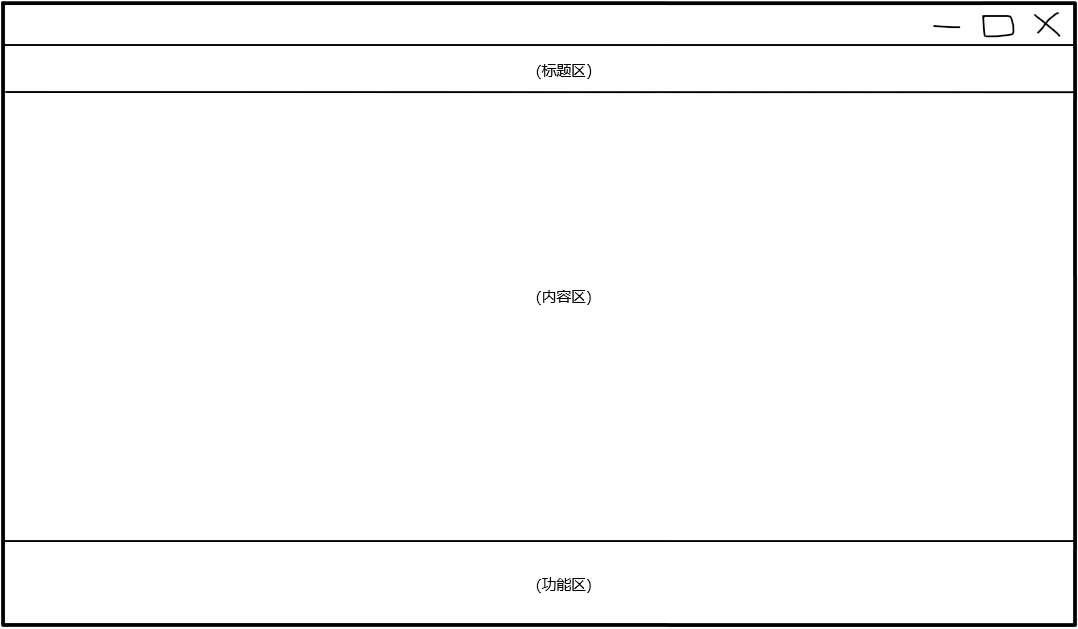
相册簿管理系统的设计和实现是一个美妙且有趣的过程。本文也将以需求分析--概要设计--详细设计--测试与维护的顺序逐步讲解设计与实现的过程。

1. 需求分析
   1. 界面的整体布局设计
      1. 构思

在界面设计这方面，java语言显然并不擅长，java的swing也因编写起来代码冗杂而长期被人诟病，而且本人在UI设计方面真心没有什么天赋，所以我遵守的设计理念就是UI尽量简洁一致，基本功能实现就行。

* + 1. 设计

从用户角度考虑，第一点，相册簿管理系统要让用户清楚地知道自己当前在哪个界面，第二点，要有一个主区域用来放置用户的相册簿集和相册簿内容，第三点，要有交互式按钮供用户使用。综上考虑，将界面分为三个区域，北区域为标题区，用来标识当前界面；中心区为内容区，用户的登录，注册，管理相册簿集和管理相册内容都在这个区域进行；南区域为功能区，顾名思义，就是一个实现各种功能的区域，并且提供交互式按钮供用户使用。具体如下图所示：

用swing里的边界布局非常容易实现上图的布局，所以让每个界面都采用这样的布局方式，这样不仅界面简洁一致，代码上也好实现。

* 1. 界面的切换与恢复
     1. 构思

有多个界面必然要设计界面的跳转，然而跳转有个问题就是要不要保留之前的界面里的内容，我觉得还是有必要的，假设用户在编辑好一页相册内容后切换到下一页编辑了，然后突然觉得上一页好像忘了编辑文字，于是想返回上一页看看，所以还是有必要实现的；用户进入相册簿和返回相册簿集这些操作，也是需要保存界面内容的，而且这两个界面的标题，内容和功能都截然不同，所以都要记录各个区域的内容以备恢复。

那么，怎么记录各个区域的内容呢？其实很简单，我们用JPanel控件来填充各个区域，JPanel是个容器，它有个特性就是你往里面加了某个控件后，这个控件就属于JPanel的一部分了，JPanel本身就具有“记忆”功能。但是在切换界面时，当前的JPanel对象会被新建的对象覆盖掉，对象一旦被覆盖便会被垃圾回收器回收再也无法找回，所以这里需要一种数据结构来保存这个即将被覆盖的对象。当需要恢复这个界面的时候再把它拉出来。

* + 1. 设计

设计一个BorderUI类，这个类存储三个区域的JPanel对象，每个JPanel对象都可以被替换；可以设置三个区域的高度比；可以更新当前界面；标题区由于只有标题文字的改变，所以采用单例模式实现。

设计一个BorderUIManager类，这个类用来管理BorderUI对象，也是为了实现界面的跳转与恢复。这个类有一个map，调用者需要给每一个BorderUI对象起一个易于记住的名字然后以String为键，以BorderUI为值将每个BorderUI存储在map中。在跳转时，要注意先在map中查询是否存在这个界面，如果没有则新建一个BorderUI并存储在map中然后跳转，如果有则直接跳转更新界面。

* 1. 代码实现与封装

1. 概要设计
2. 详细设计
3. 测试与维护

**本科毕业论文(设计)任务书**

|  |  |  |  |
| --- | --- | --- | --- |
| **学 院** | 医学技术学院 | **专 业** | 18级计算机科学与技术专升本 |
| **姓 名** | 胡立哲 | **学 号** | 201812243102012 |
| **指导老师** | 李懿 | **职 称** | 讲师 |
| **合作老师** |  | **职 称** |  |
| **题 目** | 相册簿管理系统的设计与实现 | | |
| **一、课题的内容和任务要求**   1. 课题内容：   设计并实现一个相册簿管理系统。   1. 任务要求：   实现界面的规范化布局，建立合理的数据库，并完成以下功能：   1. 设计并实现用户管理模块，用户有唯一用户名，密码，性别，出生日期，用户的相册簿。用户除了自己的唯一用户名无法修改以外，其他均可以修改。 2. 设计并实现UI管理模块。客户端在切换界面时能保存好上一个界面的“现场”以便切换回来。 3. 设计并实现相册集管理模块。相册簿有主题名，作者，可被用户新建，编辑，和删除。 4. 设计并实现相册页处理模块。用户可以任意编辑自己的相册页，可以往相册页上放置文字和图片，摆放位置可以由用户决定。对于每个文字或图片，用户都可以对其进行管理。 | | | |

|  |
| --- |
| **二、进度安排（**起止时间：2019年10月1日 ～ 2020年5月15日**）**  2019.9.27前完成开题报告，任务书和文献综述并完成开题工作  2020.2.24前完成课题的外文翻译，完成毕业设计中期检查  2020.5.4前完成毕业设计课题相关的设计，完成毕业设计论文并查重  2020.5.15前完成毕业设计论文答辩，成绩评定等工作  **三、主要参考资料**  [1] 金良磊. 化繁为简，巧用Windows 10自制电子相册[J]. 电脑知识与技术：经验技巧，2019，（7）  [2] 张志成，王鹏非. 基于stm32单片机的电子相册[J]. 电子技术与软件工程，2016，（4）  [3] 陈金立，高超. 基于TFT显示屏的电子相册设计[J]. 自动化技术与应用，2013，（11）  [4] 康志辉，曾伟渊. 电子相册管理系统设计[J]. 电脑编程技巧与维护，2015，（16）  [5] 戴明儒，陆启军. 基于php技术的电子相册系统分析与设计[J]. 计算机光盘软件与应用，2013，（22）  [6] 禹晨，陆洲. 基于java的电子相册系统的可视化开发与应用[J]，2015，（12）  [7] 燕丽红，林志雄，杨星. 基于Windows 7操作系统和Qt技术的电子相册设计[J]. 现代电子技术，2014，（8）  [8] 张伟. Premiere在音乐电子相册上的开发与应用[J]. 教育教学论坛，2019，（21）  [9] [Karim Abouelmehdi](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7" \l "auth-1). Big healthcare data: preserving security and privacy[J]. [Journal of Big Data](https://link.springer.xilesou.top/journal/40537),2018, (5)  [10] [Leonardo B. Oliveira](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "auth-1). The computer for the 21st century: present security & privacy challenges[J]. [Journal of Internet Services and Applications](https://jisajournal.springeropen.com/),2018(24)  [11] 朱平哲. 计算机网络信息安全中数据加密技术的分析[J]. 电脑知识与技术，2019 （36）：24-25  **签名栏：**  学生： 指导老师： 专业负责人：  **注意：**  1．任务书由指导老师填写、专业负责人审核，学生、指导老师、专业负责人均应签字。  2．此任务书要求在毕业论文（设计）工作开始前下达。 |

**本科毕业论文(设计)开题报告**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **学 院** | 医学技术学院 | | | **专 业** | | 18级计算机科学与技术专升本 | | |
| **姓 名** | 胡立哲 | | | **学 号** | | 201812243102012 | | |
| **指导老师** | 李懿 | | | **职 称** | | 讲师 | | |
| **合作老师** |  | | | **职 称** | |  | | |
| **题 目** | 相册簿管理系统的设计与实现 | | | | | | | |
| **题目性质** | 实验研究 | 技术开发 | 工程设计 | | 应用型√ | | 调查型 | 其他 |
| 一、选题依据和目标  （该研究的目的、意义、国内外研究现状及发展趋势）  **该研究的目的及意义**  19世纪，人类有一项伟大的创举就是发明了摄影术，从此出现了可以记录这个世界瞬间的照片。人们追求更高质量的照片和更好的摄影术，因此出现了彩色照片，高分辨率照片，摄像机也从老式照相机到单反再到现在的智能手机。然而，整理照片一直是一件麻烦的事情。上个世纪，人们整理照片的方式就是将照片整理在一本册子里因此得名“相册簿”，现在，人们的大多数照片会存储在电子设备中，无法再将照片存储在实体的册子里。为了解决这个问题，本课题旨在利用数据库技术研发出一款可以让用户存储和管理电子照片的相册簿管理系统。  以往的相册簿有一个缺点是只能放照片而无法附上文字信息，而电子相册簿可以轻松解决这个问题。另外，当人们想要起另一个主题的相册簿时，只能再去买一个相册簿，所以如果不是很有必要人们也不会花钱做麻烦事，但相册簿管理系统只是让用户单击一个按钮，导入一张照片这些简单易懂的操作便能解决上述问题，大大降低了人力成本和金钱成本。  **国内外研究现状**  在国内，已经有各式各样的制作电子相册的方式。比如，有人研究出如何用win10系统自动工具制作电子相册，在win10系统里找到“照片”应用打开，将手机中的照片导入到“照片”应用中，在该应用的右上角有一个“创建”按钮，通过创建一个“自定义视频”来开始制作你的电子相册。也有人使用单片机技术制作出一个小型数码相册，有以STM32为核心，通过硬件电路和软件设计来制作出一个完整的系统的，也有利用STC单时钟单片机，TFT-LCD彩屏和SD卡等器件来实现电子相册的。也有人使用当前互联网流行的B/S架构以及流行的框架如Struts框架来制作一个网页版的电子相册，也有基于php技术设计开发的电子相册系统。还有人在桌面应用端开发电子相册，比如使用java，以derby数据库为支持，通过eclipse软件运行，实现了基于java的电子相册的可视化开发，还有人开发基于Windows 7操作系统和Qt技术的电子相册。甚至有人利用专门的多媒体音视频制作软件来制作音乐电子相册，比如说Premiere。总的来说，制作电子相册的方式五花八门，但都有各自的优缺点。  在国外，也出现了各式各样的电子相册，其中比较有名的比如Google网络相册Picasa Tool Pro，这是一款很简洁，精致，好用的相册管理工具，你可以制作自己的相册然后将你的相册共享至你的google+圈子。还有web端应用imagevue，这是个国外比较有名的具有Flash幻灯效果的在线相册网站程序，你可以用他制作一个完整照片或图片展示网站，你也可以把它做为一个画廊、相册整合嵌入到您现有的网站里去。  **发展趋势**  电子相册分为两种，一种是软件类型的电子相册，一种是硬件类型的电子相册。windows media player等制作的电子相册，都属于软件类型，除此之外，还有一种电子相册为硬件类型，指能够不借助电脑可以在LCD面板上显示数码照片的电子产品的展示效果，还能够将照片显示到电视机上。还可接U盘、SD卡、MMC卡，除播放图片外，还可播放MP3、内置左右双喇叭、边播放图片边听MP3、看手机AVI格式电影、DAT格式或[MPEG格式](https://baike.baidu.com/item/MPEG%E6%A0%BC%E5%BC%8F" \t "https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E7%9B%B8%E5%86%8C/_blank)或MPG格式电影（VCD文件）、VOB格式电影（DVD文件）（其它不支持的格式可以软件转换）、输出音频视频到电视机或音响，制作这种电子相册的产品称为电子相框，《电子工程杂志》将电子相框分为3类，简易电子相框、“多媒体”电子相框高级、“多媒体”电子相框。  简易数码相框只能显示[JPEG格式](https://baike.baidu.com/item/JPEG%E6%A0%BC%E5%BC%8F" \t "https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E7%9B%B8%E5%86%8C/_blank)的图片，而多媒体数码相框则可以播放音乐和视频。 某些高级“多媒体”数码相框可以通过因特网从RSS、照片共享网站甚至电子邮件下载图片。这些型号通常也支持无线传输 （IEEE802.11）。大部分数码相框可以像幻灯一样按可调整的时间间隔显示图片。一些相框还可以播放MP3音乐或者用相机拍摄的视频片断，比如MPEG文件。  数码摄影必然推动电子相框的发展，因为全世界打印的数码相片不到35%。数码相框通常直接插上相机的存储卡展示照片，当然更多的数码相框会提供内部存储空间以接外接存储卡功能。数码相框就是一个相框，不过它不再用放进相片的方式来展示，而是通过一个液晶的屏幕显示，它可以通过读卡器的接口从SD卡获取相片，并设置循环显示的方式，比普通的相框更灵活多变，也给现在日益使用的数码相片一个新的展示空间。 | | | | | | | | |

|  |
| --- |
| 二、课题关键问题及难点  关键问题   1. 采用哪种数据存储的方式？ 2. 如何实现界面的切换？ 3. 如何实现控件的拖动？ 4. 如何从控件中提取关键数据存储以及读取关键数据来生成控件？   难点   1. 每个用户有自己的相册簿集，每个相册簿里又有若干页，每一页里又有若干文字和图片，程序如何管理好每个用户的这些相册簿使之能有序存储和加载？   三、完成该课题研究已具备的条件（有关的研究工作基础，仪器设备条件，经费情况）  一台笔记本电脑,eclipse。无需经费。  四、研究方案  1. 拟采取的研究方法或试验方法及主要技术路线  研究方法   1. 对需求进行分析，确定程序设计语言，IDE，程序功能和数据存储方式。 2. 查找相关的文献资料，并且与导师沟通。 3. 根据所搜集资料，对程序功能进行模块划分和概要设计。 4. 开始具体实现各个构件及模块。实现各个模块中的基本功能。 5. 模块集成并测试，如有bug则修理。 6. 在4)的基础上完成所有功能并集成测试，如有bug则修复。   主要技术路线  由于决定目标平台为PC，所以决定采用java语言利用javase基础库如swing来做界面，utils等来做基础逻辑实现，用第三方库fastjson来做用户数据存储。  2. 研究进度安排  1.分析程序需求，确定采用的技术方案（1周）  1.对程序功能进行分析并规划模块，进行该程序的概要设计（2周）  2.实现各个模块内的功能并给出必要的接口供模块间交互。（3周）  3.对每个模块进行单元测试（1周）  4.修改bug，以及对性能表现不佳的地方进行性能优化，集成测试（1周）  5.修改bug直至满足要求，交付程序（1周）  **五、**参考文献  [1] 金良磊. 化繁为简，巧用Windows 10自制电子相册[J]. 电脑知识与技术：经验技巧，2019，（7）  [2] 张志成，王鹏非. 基于stm32单片机的电子相册[J]. 电子技术与软件工程，2016，（4）  [3] 陈金立，高超. 基于TFT显示屏的电子相册设计[J]. 自动化技术与应用，2013，（11）  [4] 康志辉，曾伟渊. 电子相册管理系统设计[J]. 电脑编程技巧与维护，2015，（16）  [5] 戴明儒，陆启军. 基于php技术的电子相册系统分析与设计[J]. 计算机光盘软件与应用，2013，（22）  [6] 禹晨，陆洲. 基于java的电子相册系统的可视化开发与应用[J]，2015，（12）  [7] 燕丽红，林志雄，杨星. 基于Windows 7操作系统和Qt技术的电子相册设计[J]. 现代电子技术，2014，（8）  [8] 张伟. Premiere在音乐电子相册上的开发与应用[J]. 教育教学论坛，2019，（21）  [9] [Karim Abouelmehdi](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7" \l "auth-1). Big healthcare data: preserving security and privacy[J]. [Journal of Big Data](https://link.springer.xilesou.top/journal/40537),2018, (5)  [10] [Leonardo B. Oliveira](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "auth-1). The computer for the 21st century: present security & privacy challenges[J]. [Journal of Internet Services and Applications](https://jisajournal.springeropen.com/),2018(24)  [11] 朱平哲. 计算机网络信息安全中数据加密技术的分析[J]. 电脑知识与技术，2019 （36）：24-25 |
| 六、指导老师意见  签名：  年 月 日 |
| 七、学院意见  学院负责人签名：  年 月 日 |

**附：开题报告会情况记录**

|  |  |  |  |
| --- | --- | --- | --- |
| **参加开题报告会的主要人员** | | | |
| **姓 名** | **职 称** | **姓 名** | **职 称** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **开题报告提出的主要问题及回答情况：**  记录人：  年 月 日 | | | |

**本科毕业论文(设计)文献综述**

|  |  |  |  |
| --- | --- | --- | --- |
| **学 院** | 医学技术学院 | **专 业** | 计算机科学与技术专升本 |
| **姓 名** | 胡立哲 | **学 号** | 201812243102012 |
| **指导老师** | 李懿 | **职 称** | 讲师 |
| **合作老师** |  | **职 称** |  |
| **题 目** | 相册簿管理系统的设计与实现 | | |

**文献综述**（主要包括国内外现状、研究方向、进展情况、存在问题、参考文献等）

**电子相册的发展浅析**

电子相册是指可以在电脑上或者是在移动端上观赏的区别于CD/VCD的静止图片的特殊软件或文档，其内容不局限于摄影照片，也可以包括各种艺术创作图片。电子相册具有传统相册无法比拟的优越性：图，文，声，像并茂的表现手法，随意修改编辑的功能，快速的检索方式，永不褪色的恒久保存特性，以及廉价复制分发的优越手段。

1.电子相册的发展历史

早期的“数码相册”与“数码”根本没有半点关系，只是影集生产商为了区别于传统影集的一个代名词。数码相册生产商将影集载体上印上各式各样的边框图形，照相馆将拍好的照片按照边框的形状裁切，然后将裁切的照片裱膜好并用双面胶把照片粘贴于相应位置形成一个情景互动的场面。因为有了情景互动，和样式多样化等原因数码相册也曾风靡一时。直到进入2000年，数码相机开始在各大型影楼相继出现，加之电脑与互联网的兴起，短短3到4年的时间，数码相机及相关产品就取代了由胶卷垄断了百余年的历史。由于数码的灵活性和后期可编辑性强，一种更新型的相册“一体相册”或称“圣经相册”也便随之兴起。从“一体”两个字我们可以大致想到这种相册做工的精细。它实现了照片与载体的有机结合，二者融为了一个有机的整体，故称“一体相册”。一体相册因为在装订时做到了整体裁切，所以就整体外形来讲比数码相册整齐，加上数码的灵活性实现了情和景的无缝结合，这种相册很快在各影楼跟风兴起，从而也推动了一体相册的发展，一体相册很快开始取代数码相册的主导地位，成为潮流。

随着IT行业的发展，出现了以电脑终端和手机终端为载体的相册。电脑终端方面，如腾讯QQ空间相册和动感影集，一种以网络和电脑为载体的相册随即兴起。空间相册是QQ用户的个人相片展示，存放的平台，所有QQ用户免费享用相册，这一变革使得用户的电子照片可以永久的保存在网络上，比数码相框前进了一大步。

随着手机系统的发展，一种在智能化时代——安卓时代下诞生的智能相册应运而生，它是一种新潮的电子相册应用。这种电子相册用全新的软件开发设计，可以多平台展示，支持IOS系统和安卓系统，用户可以选择自己喜欢的固定的成套模板，也可以选择自己喜欢的不同风格的模板自由组合，还可以“量身定制”，要求设计独一无二的专属的模板或者原创音乐。这种相册更具互动性，灵活性，携带方便。可以让自己的相册有声有色，优美的音乐，即使在没有网络的环境下也能随心所欲的制作电子相册，让用户真正成为生活的艺术家。

2.国内外现状

在国内，已经有各式各样的制作电子相册的方式。比如，有人研究出如何用win10系统自动工具制作电子相册[[[1]](#footnote-0)]，在win10系统里找到“照片”应用打开，将手机中的照片导入到“照片”应用中，在该应用的右上角有一个“创建”按钮，通过创建一个“自定义视频”来开始制作你的电子相册。也有人使用单片机技术制作出一个小型数码相册，有以STM32为核心，通过硬件电路和软件设计来制作出一个完整的系统的[[[2]](#footnote-1)]，也有利用STC单时钟单片机，TFT-LCD彩屏和SD卡等器件来实现电子相册的[[[3]](#footnote-2)]。也有人使用当前互联网流行的B/S架构以及流行的框架如Struts框架来制作一个网页版的电子相册[[[4]](#footnote-3)]，也有基于php技术设计开发的电子相册系统[[[5]](#footnote-4)]。还有人在桌面应用端开发电子相册，比如使用java，以derby数据库为支持，通过eclipse软件运行，实现了基于java的电子相册的可视化开发[[[6]](#footnote-5)]，还有人开发基于Windows 7操作系统和Qt技术的电子相册[[[7]](#footnote-6)]。甚至有人利用专门的多媒体音视频制作软件来制作音乐电子相册，比如说Premiere[[[8]](#footnote-7)]。总的来说，制作电子相册的方式五花八门，但都有各自的优缺点。

在国外，也出现了各式各样的电子相册，其中比较有名的比如Google网络相册Picasa Tool Pro，这是一款很简洁，精致，好用的相册管理工具，你可以制作自己的相册然后将你的相册共享至你的google+圈子。还有web端应用imagevue，这是个国外比较有名的具有Flash幻灯效果的在线相册网站程序，你可以用他制作一个完整照片或图片展示网站，你也可以把它做为一个画廊、相册整合嵌入到您现有的网站里去。

3.存在的问题及改进

虽然国内有各种样式的电子相册，但都有各自的缺点。利用windows系统自带工具制作的电子相册，首先，它繁琐的步骤就决定了不适合用户使用，其次，自带工具的功能有限，无法让用户自由发挥创作，还有，照片只能存储在本机上也是个很大的弊端。然后对于利用单片机开发的电子相册系统，有一个很大的弊端是单片机的存储容量通常不会很大，当用户存储照片和文字到一定量时，就必须删除一些才能够容纳新的照片进来，如何解决容量问题是一个瓶颈。对于web端，采用B/S架构确实可以解决容量问题，但网站有一个弊端就是一些网站可能隐藏着病毒，甚至本身就是钓鱼网站，正是因为有这样的网站的存在，导致了用户不敢轻易往网站上提交自己的私人照片或私人信息。所以，最合理的平台是桌面应用端或者移动端。

本系统采用的就是桌面应用端。桌面应用一方面方便了人们的操作，另一方面减少了人们对网络安全的顾虑。在这个大数据时代，安全和隐私是重要问题。隐私的定义是能够保护有关个人可识别的敏感信息。它侧重于个人数据的使用和管理，如制定政策和制定授权要求。安全性的定义是防止未经授权的访问。它侧重于保护数据免受恶意攻击和窃取数据以牟利。[[[9]](#footnote-8)]为了加强软件的安全性，本系统对用户密码进行了加密处理。因此，我们先对数据加密这件事情进行初步的认识。

在使用数据加密技术对网络信息数据进行保护使用的时候，最基础的密钥算法就是对称密钥与非对称密钥的使用。对称密钥，就是指使用相同的一个密钥，可以同时对网络信息数据进行加密和解密。非对称密钥，与对称密钥刚好相反，就是在进行网络信息数据加密与解密的过程中，需要使用不同的密钥来处理。也因为不同的算法，会产生不同种类的数据加密技术。事实上，现在已经有了许多类型的加密技术[[[10]](#footnote-9)]，下面介绍几种比较常见的。

* 端端加密技术

端端加密技术，就是指在传递数据前，对信息数据进行加密，直接传递相对应的密文数据，接收方接收到密文后，再使用相对应的密钥对接收的密文进行解密，从而获得需要的数据信息。端端加密技术的优点是使用的价格相对便宜，物美价廉。而且，数据在传递的时候，是两端进行加密，解密，更好地保证了信息数据的安全性。

* 节点加密技术

节点加密技术，就是指借助链路为技术的载体，通过每一个节点，对要传递的信息数据进行加密和解密。然而，虽然在通信的节点处，会有一个相对安全的区域，而且信息数据也是以密文的形式进行传递的，但是数据加密与解密的过程中，是在各自的安全区域内进行的，相对而言过于简单，容易被别人破解，获得密文背后的信息数据。[[[11]](#footnote-10)]

* 链路加密技术

链路加密技术，顾名思义，也是以链路为载体，信息数据在进行传递的时候，也是以密文的形式进行传递的，而且在信息传递的过程中，信息数据会进行反复的加密与解密，并且这个过程覆盖了整个传输路径之中，相对于节点加密技术，更具有安全性，对信息数据的安全保护作用也更好。

由于本系统只对用户密码进行加密，在用户提交密码后只需加密存储到数据库中而不需要解密，所以采用非对称加密的算法，比如当今广泛使用的MD5信息摘要算法。MD5算法很好地解决了用户的账户安全问题，因为它可以将任意长度的输入串经过计算得到固定长度的输出，而且只有在明文相同的情况下，才能等到相同的密文，并且这个算法是不可逆的，即便得到了加密以后的密文，也不可能通过解密算法反算出明文。这样就可以把用户的密码以MD5值的方式保存起来，用户登录的时候，系统是把用户输入的密码计算成 MD5 值，然后再去和系统中保存的 MD5 值进行比较，如果密文相同，就可以认定密码是正确的，否则密码错误。通过这样的步骤，系统在并不知道用户密码明码的情况下就可以确定用户登录系统的合法性。这样不但可以避免用户的密码被具有系统管理员权限的用户知道，而且还在一定程度上增加了密码被破解的难度。

4.参考文献

[1] 金良磊. 化繁为简，巧用Windows 10自制电子相册[J]. 电脑知识与技术：经验技巧，2019，（7）

[2] 张志成，王鹏非. 基于stm32单片机的电子相册[J]. 电子技术与软件工程，2016，（4）

[3] 陈金立，高超. 基于TFT显示屏的电子相册设计[J]. 自动化技术与应用，2013，（11）

[4] 康志辉，曾伟渊. 电子相册管理系统设计[J]. 电脑编程技巧与维护，2015，（16）

[5] 戴明儒，陆启军. 基于php技术的电子相册系统分析与设计[J]. 计算机光盘软件与应用，2013，（22）

[6] 禹晨，陆洲. 基于java的电子相册系统的可视化开发与应用[J]，2015，（12）

[7] 燕丽红，林志雄，杨星. 基于Windows 7操作系统和Qt技术的电子相册设计[J]. 现代电子技术，2014，（8）

[8] 张伟. Premiere在音乐电子相册上的开发与应用[J]. 教育教学论坛，2019，（21）

[9] [Karim Abouelmehdi](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7" \l "auth-1). Big healthcare data: preserving security and privacy[J]. [Journal of Big Data](https://link.springer.xilesou.top/journal/40537),2018, (5)

[10] [Leonardo B. Oliveira](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "auth-1). The computer for the 21st century: present security & privacy challenges[J]. [Journal of Internet Services and Applications](https://jisajournal.springeropen.com/),2018(24)

[11] 朱平哲. 计算机网络信息安全中数据加密技术的分析[J]. 电脑知识与技术，2019 （36）：24-25

**本科毕业论文(设计)外文翻译**

|  |  |  |  |
| --- | --- | --- | --- |
| **学 院** | 医学技术学院 | **专 业** | 18计算机科学与技术专升本 |
| **姓 名** | 胡立哲 | **学 号** | 201812243102012 |
| **指导老师** | 李懿 | **职 称** | 讲师 |
| **合作老师** |  | **职 称** |  |
| **题 目** | 相册簿管理系统 | | |

**译文：**

**大医疗保健数据：维护安全和隐私**

大数据期刊，第5卷，文章编号：1（2018)

**摘要**

大数据从根本上改变了组织管理、分析和利用任何行业数据的方式。最有前途的领域之一，其中大数据可以应用进行更改是医疗保健。大医疗保健数据在改善患者结果、预测疫情爆发、获得有价值的见解、避免可预防的疾病、降低医疗保健交付成本以及提高总体生活质量方面具有相当大的潜力。但是，在维护安全性和患者隐私权的同时，决定数据的允许用途是一项艰巨的任务。大数据，无论对医学科学的进步多么有用，并且对所有医疗保健组织的成功至关重要，只有解决安全和隐私问题，才能使用大数据。为了确保安全和值得信赖的大数据环境，必须确定现有解决方案的局限性，并为未来的研究设想方向。在本文中，我们调查了适用于医疗保健行业的大数据中最先进的安全和隐私挑战，评估了在出现大医疗保健数据时如何发生安全和隐私问题，并讨论了如何解决这些问题的方法。我们主要关注最近提出的基于匿名化和加密的方法，比较其优点和局限性，并设想了未来的研究方向。

**介绍**

变革是全球医疗行业的新准则。事实上，在可预见的将来，健康和患者数据数字化在临床、运营和商业模式以及一般经济世界中正在发生巨大和根本性的变化。人口老龄化和生活方式的改变推动了这一转变;软件应用程序和移动设备的激增;创新的疗法;更加注重护理质量和价值;循证医学，而不是主观的临床决定，所有这些都导致提供重大的机会，以支持临床决策，改善医疗保健提供，管理和政策制定，监测疾病，监测不良事件，并优化治疗影响多个器官系统的疾病[[1](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR1" \o "Burghard C. Big data and analytics key to accountable care success. Framingham: IDC Health Insights; 2012.)，[2](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR2" \o "Fernandes L, O’Connor M, Weaver V. Big data, bigger outcomes. J AHIMA. 2012;83:38–42.)]。

如上所述，医疗保健领域的大数据分析具有许多好处、承诺，并带来了巨大的变革医疗保健的潜力，但它也带来了多种障碍和挑战。事实上，对大型医疗保健数据安全和隐私的担忧逐年增加。此外，医疗保健组织发现，确定安全和隐私要求时采用被动的、自下而上、以技术为中心的方法不足以保护组织及其患者[[3]](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR3" \o "David Houlding, MSc, CISSP. Health Information at Risk: Successful Strategies for Healthcare Security and Privacy. Healthcare IT Program Of ce Intel Corporation, white paper. 2011.)。

因此，需要新的信息系统和方法来防止敏感信息和其他类型的安全事件的泄露，以便有效利用大医疗保健数据。

在本文中，我们讨论了一些有趣的相关工作，并呈现了大健康数据安全的风险，以及一些新技术来纠正这些风险。然后，我们重点关注医疗保健领域的大数据隐私问题，提及不同监管机构制定的各种法律和法规，并指出一些用于确保患者隐私的可行技术。此后，我们提供一些在文献中报告的一些建议技术和方法，以处理医疗保健中的安全和隐私风险，同时确定其局限性。最后，我们提出结论，并突出未来方向。

**成功的相关工作**

无缝集成各种大型医疗保健数据技术，不仅可以让我们更深入地了解临床和组织流程，还能促进更快、更安全的患者吞吐量，并提高效率和帮助改善患者流量、安全性、护理质量和整体患者体验，无论成本如何。

南泰恩赛德NHS基金会信托基金就是如此，该基金会是英格兰东北部的急性和社区卫生服务机构，它了解始终为患者提供高质量、安全和富有同情心的护理的重要性，但需要更好地了解其医院的运作方式，以改善资源分配和等待时间，并确保及早发现任何问题并采取行动[[4]。](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR4" \o "South Tyneside NHS Foundation Trust. Harnessing analytics for strategic planning, operational decision making and end-to-end improvements in patient care. IBM Smarter Planet brief. 2013.)

另一个例子是UNC医疗保健（UNCHC），这是北卡罗来纳州的一个非营利性综合医疗保健系统，它实施了一个新的系统，允许临床医生使用自然语言处理快速访问和分析非结构化患者数据。事实上，UNCHC已经访问并分析了患者医疗记录中的大量非结构化内容，以提取及时干预的再入院风险的见解和预测，为高危患者提供更安全的护理，并减少再入院[[5](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR5" \o "UNC Health Care relies on analytics to better manage medical data and improve patient care. IBM Press release. 2013.)]。

此外，在美国，印第安纳州健康信息交换，这是一个非盈利组织，提供了一个安全而强大的卫生信息网络，连接印第安纳州的90多家医院，社区卫生诊所，康复中心和其他医疗保健提供者。它允许医疗信息跟踪病人托管在一个医生办公室或只在医院系统[[6](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR6" \o )]。

一个例子是位于加州的凯撒永久医疗网络。它拥有超过 900 万成员，估计可管理从 26.5 PB 到 44 PB 的大量数据[[7](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR7" \o "Transforming healthcare through big data, strategies for leveraging big data in the healthcare industry. Institute for Health. 2013.)]。

大数据分析在加拿大也使用，例如多伦多的婴儿医院。这家医院成功地改善了容易严重感染的新生儿的疗效。另一个例子是Artemis项目，这是一个新生儿监测平台，旨在配合IBM和安大略省理工学院之间的合作。它支持获取和存储患者的生理数据和临床信息系统数据，实现在线和实时分析、回顾性分析和数据挖掘[[8](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR8" \o )]的目标。

在欧洲和意大利，意大利药品代理收集和分析大量有关昂贵新药的临床数据，作为国家盈利计划的一部分。根据结果，它可能会重新评估药品价格和市场准入条件[[9](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR9" \o "Groves P, Kayyali B, Knott D, Kuiken SV. The big data revolution in healthcare, accelerating value and innovation. 2013.)]。

在移动医疗领域，世界卫生组织在塞内加尔启动了"健康移动"项目，并在mDiabetes倡议下支持各国建立使用移动技术，特别是短信和应用的大型项目，以控制、预防和管理糖尿病、癌症和心脏病等非传染性疾病[[10]](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR10" \o "WHO. Mobile phones help people with diabetes to manage fasting and feasting during Ramadan. Features. 2014.)。mDiabetes 是利用广泛的移动技术向数百万塞内加尔人提供健康信息并扩大获得专业知识和护理的机会的第一个举措。该举措于2013年在哥斯达黎加启动，被正式选定为第一个国家，目前正在致力于一项预防吸烟和帮助吸烟者戒烟的戒烟计划，这是赞比亚的一个乳腺癌项目，并计划在其他国家推行高血压和mhealth计划。

继欧洲、加拿大、澳大利亚、俄罗斯和拉丁美洲之后，数据驱动医学的全球领导者索菲亚遗传学公司（Sophia Genetics）在最近举行的美国医学遗传学和基因组学院（ACMG）2017年年会上宣布，其人工智能已被非洲医院采用，以推进整个非洲大陆的患者护理[[12](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR12" \o )]。

例如，在摩洛哥，卡萨布兰卡的PharmaProcess、ImmCell、Al Azhar肿瘤中心和拉巴特的里亚德生物学中心是一些处于创新前沿的医疗机构，它们已经开始整合索菲亚，以加速和分析基因组数据，以识别患者基因组谱型中的致病突变，并决定最有效的护理。作为 SOPHIA 的新用户，他们成为 46 个国家/地区 260 家医院组成的大型网络的一部分，这些医院在患者病例和患者群体中共享临床见解，为生物医学发现的知识库提供依据，以加快诊断和护理。

虽然自动化已导致改善患者护理工作流程和降低成本，但它也在增加医疗保健数据，以增加安全和隐私泄露的可能性。2016 年，CynergisTek 发布了 Redspin 的第 7 份年度违规报告：保护健康信息 （PHI）[[13]](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR13" \o "CynergisTek, Redspin. «BREACH REPORT 2016: Protected Health Information (PHI)» 2017.)其中报告，2016 年针对医疗保健提供商的黑客攻击增加了 320%，2016 年 81% 的被违反记录是主要由黑客攻击造成的。此外，勒索软件被定义为一种恶意软件，它加密数据并劫持数据，直到满足赎金需求，已被确定为对医院最严重的威胁。本报告的其他调查结果包括：

* 325 起大规模违反 PHI 的行为，危害了 16，612，985 例患者记录。
* 在今年最大的一次事件中，有3，620，000人违反了病人记录。
* 40% 的大型违规事件涉及未经授权的访问/披露。

这些发现表明，提供商迫切需要采取更积极和全面的方法来保护其信息资产，并应对网络攻击对医疗保健日益增长的威胁。

几个繁荣的举措似乎帮助医疗保健行业不断提高其保护患者信息的能力。例如，2014年1月，由奥巴马总统的顾问约翰·波德斯塔领导的白宫对大数据和隐私进行了90天的审查。审查提出了具体建议，以最大化大数据的利益和最小化风险[[14，](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR14" \o "Podesta J, et al. Big data: seizing opportunities, preserving values. Executive Office of the President. 2014;1:2013.) [15](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR15" \o "House W. Big data and privacy: a technological perspective. Washington: Executive Office of the President, President’s Council of Advisors on Science and Technology; 2014.)]，即：

* 政策应更多地关注大数据的实际使用，而较少关注大数据的收集和分析。此类现有策略不太可能产生改善隐私的有效策略，或随着时间的推移可扩展。
* 有关隐私保护的政策应该解决目的，而不是规定机制。
* 需要研究有助于保护隐私的技术、影响隐私保护行为的社会机制，以及能够促进技术变革并在经济机会之间创造适当平衡的法律选择，国家优先事项和隐私保护。
* 增加有关隐私保护的教育和培训机会，包括专业人员的职业道路。提供导致隐私专业知识的教育的计划至关重要，需要鼓励。
* 隐私保护应扩大到非美国公民，因为隐私是一项全球价值，应反映在联邦政府如何处理非美国公民的个人身份信息上[[16]。](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR16" \o "House W. FACT SHEET: big data and privacy working group review. 2014.)

经合组织卫生保健质量指标（HCQI）项目负责2013/2014年一项计划，以开发工具，协助各国平衡数据隐私风险和未开发和使用健康数据的风险。该计划包括制定不同类型和数据用途的风险分类，以及各国为减少直接影响每个人日常生活的风险和实现数据使用而可以采用的有希望的做法[[17]。](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR17" \o "OECD. Data-driven healthcare innovation, management and policy, DELSA/HEA(2013)13. Paris: OECD; 2013.)

**大数据中的隐私和安全问题**

大数据的安全和隐私是重要问题。隐私通常被定义为能够保护有关个人可识别的医疗保健信息的敏感信息。它侧重于个人个人数据的使用和管理，如制定政策和制定授权要求，以确保患者的个人信息以正确的方式收集、共享和使用。虽然安全性通常定义为防止未经授权的访问，但有些则包括明确提及完整性和可用性。它侧重于保护数据免受恶意攻击和窃取数据以牟利。虽然安全性对于保护数据至关重要，但它不足以解决隐私问题。表[1](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab1)侧重于安全性和隐私之间的其他差异。

表1

### **大医疗保健数据的安全性**

虽然医疗保健组织存储、维护和传输大量数据以支持提供高效和适当的医疗服务，但缺点是缺乏技术支持和安全性极小。使问题复杂化的是，医疗保健行业仍然是最容易发生公开披露的数据泄露的行业之一。事实上，攻击者可以使用数据挖掘方法和过程来查找敏感数据并将其发布给公众，从而发生数据泄露。虽然实施安全措施仍是一个复杂的过程，但随着击败安全控制的方法变得更加复杂，风险不断增加。

因此，组织实施医疗保健数据安全解决方案至关重要，这些解决方案将保护重要资产，同时满足医疗保健合规性要求。

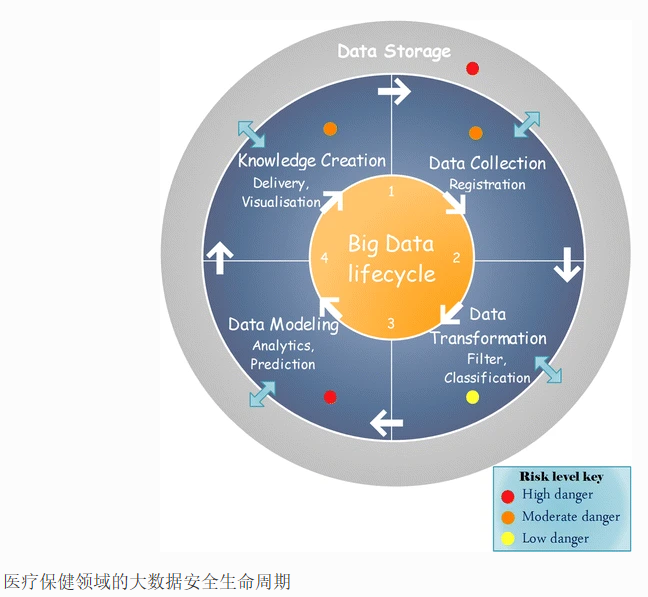
1. 大数据安全生命周期

在安全和隐私方面，Kim[等人认为大数据](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR18" \o )的安全性涉及三个问题：数据安全、访问控制和信息安全。在这方面，医疗保健组织必须实施安全措施和方法，以保护其大数据、相关硬件和软件以及临床和管理信息免受内部和外部风险的影响。在项目开始时，必须建立数据生命周期，以确保就历史或新数据的保留、成本效益、重用和审计做出适当的决策[[19]](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR19" \o "\“Data-driven healthcare organizations use big data analytics for big gains\” IBM white paper February. 2013.)。

Yazan等人[[20](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR20" \o "Yazan A, Yong W, Raj Kumar N. Big data life cycle: threats and security model. In: 21st Americas conference on information systems. 2015.)] 建议从 Xu 等人扩展的大数据安全生命周期模型此模型旨在解决大数据生命周期的各个阶段，并将在这些阶段中面临大数据环境的威胁和攻击关联起来，而 则从用户角色的角度处理大数据生命周期：数据提供程序、数据收集器、数据挖掘者和决策者。在中提出的模型由四个互连阶段组成：数据收集阶段、数据存储阶段、数据处理和分析以及知识创建。

此外，CCW（慢性疾病数据仓库）遵循正式的信息安全生命周期模型，该模型由四个核心阶段组成，用于识别、评估、保护和监控患者数据安全威胁。这种生命周期模型正在不断改进，重点是持续关注和持续监控 [[21](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR21" \o )] 。

在本文中，我们建议一个模型，将[[20]](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR20" \o "Yazan A, Yong W, Raj Kumar N. Big data life cycle: threats and security model. In: 21st Americas conference on information systems. 2015.)中介绍的阶段和 [[21]](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR21" \o )中提及的阶段结合起来，以便提供包含策略和机制，以确保在大数据生命周期的每个步骤中解决威胁和攻击。图[1](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Fig1)显示了医疗保健大数据生命周期中的主要元素。

图1

* 数据收集阶段这是显而易见的第一步。它涉及以不同格式从不同来源收集数据。从安全角度来看，保护大健康数据技术是生命周期第一阶段的必要要求。因此，从可信来源收集数据、保护患者隐私（不得尝试识别数据库中的单个患者）并确保此阶段得到保护和保护非常重要。事实上，必须采用一些成熟的安全措施，以确保所有数据和信息系统都受到保护，防止未经授权的访问、披露、修改、复制、转移、销毁、丢失、误用或盗窃。
* 数据转换阶段数据可用后，第一步是根据数据的结构对数据进行筛选和分类，并进行任何必要的转换，以便执行有意义的分析。更广泛地说，需要数据过滤、扩充和转换，以提高数据在分析或建模阶段之前的质量，并删除或适当地处理噪声、离群值、缺失值、重复数据实例等。另一方面，收集的数据可能包含敏感信息，这使得在数据转换和存储过程中采取足够的预防措施变得极其重要。为了保证收集的数据的安全，数据应保持隔离和保护，方法是维护访问级安全和访问控制（利用大量目录和数据库列表作为用户凭据、应用程序登录模板、密码策略和客户端设置的中央存储库[）[22]，](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR22" \o )并定义一些安全措施，如数据匿名化方法、排列和数据分区。
* 数据建模阶段一旦数据被收集、转换并存储在安全的存储解决方案中，就会执行数据处理分析以生成有用的知识。在此阶段，可以采用受监督的数据挖掘技术（如聚类、分类和关联）进行特征选择和预测建模。此外，还有一些学习技术组合，提高了最终模型的准确性和鲁棒性。另一方面，提供安全的处理环境至关重要。事实上，此阶段的数据挖掘人员的重点是使用强大的数据挖掘算法来提取敏感数据。因此，数据挖掘过程和网络组件一般必须配置和保护，以防止基于数据挖掘的攻击和可能发生的任何安全漏洞，并确保只有经过授权的员工在此阶段工作。此过程有助于消除某些漏洞，并将其他漏洞缓解到较低风险级别。
* 知识创造阶段最后，建模阶段提供了新的信息和有价值的知识供决策者使用。这些创建的知识被视为敏感数据，尤其是在竞争环境中。事实上，医疗保健组织意识到其敏感数据（例如患者个人数据）不会公开发布。因此，安全遵守和核查是这一阶段的主要目标。

在大数据生命周期的所有阶段，它都需要数据存储、数据完整性和数据访问控制。

1. 正在使用的技术

各种技术正在使用，以确保大医疗保健数据的安全性和隐私性。最广泛使用的技术包括：

1. 认证认证是证明或确认被认证人或被认证人所作的或关于被认证人的主张真实、可信的行为。它在任何组织内都发挥着至关重要的作用：保护对公司网络的访问，保护用户的身份，并确保用户真正成为他假装的样子。

信息身份验证可能会带来特殊问题，尤其是中间人 （MITM） 攻击。大多数加密协议包括某种形式的端点身份验证，专门用于防止 MITM 攻击。例如 ，[传输](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR23" \o "Zhang R, Liu L. Security models and requirements for healthcare application clouds. In: IEEE 3rd international conference on cloud computing. 2010.)层安全 （TLS） 及其前身安全套接字层 （SSL） 是加密协议，为 Internet 等网络的通信提供安全。TLS 和 SSL 端到端地加密传输层中的网络连接段。该协议的几个版本在 Web 浏览、电子邮件、互联网传真、即时消息和 IP 语音（VoIP ）等应用中广泛使用。可以使用 SSL 或 TLS 使用相互信任的证书颁发机构对服务器进行身份验证。还可以实现基于票证授予票证或服务票证的哈希技术，如 SHA-256[[24](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR24" \o "Shafer J, Rixner S, Cox AL. The hadoop distributed filesystem: balancing portability and performance. In: Proceedings of 2010 IEEE international symposium on performance analysis of systems & software (ISPASS), March 2010, White Plain, NY. p. 122–33.)]和 Kerberos 机制，以实现身份验证。此外，牛眼算法可用于监控 360° 中的所有敏感信息。该算法用于确保数据安全并管理原始数据和复制数据之间的关系。也只允许授权人员读取或写入关键数据。论文 [[25](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR25" \o "Yang C, Lin W, Liu M. A novel triple encryption scheme for hadoop-based cloud data security. In: Emerging intelligent data and web technologies (EIDWT), 2013 fourth international conference on. 2013. p. 437–42.)] 提出了一种使用单时垫算法的新颖而简单的身份验证模型。它提供删除服务器之间的密码通信。在医疗保健系统中，提供者提供的医疗保健信息和消费者的身份都应在每次访问时进行验证。

1. 加密数据加密是防止未经授权访问敏感数据的有效手段。其解决方案保护和维护数据在其整个生命周期（从数据中心到端点（包括医生、临床医生和管理员使用的移动设备）以及云中的数据所有权。加密对于避免出现数据包嗅探和存储设备被盗等漏洞非常有用。医疗保健组织或提供商必须确保加密方案高效、患者和医疗保健专业人员都易于使用，并且易于扩展以包括新的电子健康记录。此外，应尽量减少每一方持有的密钥数。

尽管各种加密算法已经开发和部署得相对较好（RSA, Rijndael, AES and RC6 [[24](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR24" \o "Shafer J, Rixner S, Cox AL. The hadoop distributed filesystem: balancing portability and performance. In: Proceedings of 2010 IEEE international symposium on performance analysis of systems & software (ISPASS), March 2010, White Plain, NY. p. 122–33.), [26](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR26" \o "Federal Information Processing Standards Publication 197. Specification for the advanced encryption standards (AES). 2001.), [27](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR27" \o "Somu N, Gangaa A, Sriram VS. Authentication service in hadoop using one time pad. Indian J Sci Technol. 2014;7:56–62.)], DES, 3DES, RC4 [[28](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR28" \o "Fluhrer S, Mantin I, Shamir A. Weakness in the key scheduling algorithm of RC4. In: 8th annual international workshop on selected areas in cryptography, London: Springer-Verlag. 2001.)], IDEA, Blowfish …），但正确选择适当的加密算法以强制实施安全存储仍然是一个难题。

1. 数据屏蔽将敏感数据元素替换为无法识别的值。它不是真正的加密技术，因此无法从屏蔽值返回原始值。它使用去识别数据集或屏蔽个人标识符（如姓名、社会保险号）的策略，以及禁止或概括准标识符（如出生日期和邮政编码）。因此，数据屏蔽是实时数据匿名化的最流行的方法之一。K-匿名最初由斯瓦尼和Samrati提出 [[29，](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR29" \o "Sweeney L. Achieving k-anonymity privacy protection using generalization and suppression. Int J Uncertain Fuzziness Knowl Based Syst. 2002;10:571–88.) [30](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR30" \o "Samrati P. Protecting respondents identities in microdata release. IEEE Trans Knowl Data Eng. 2001;13:1010–27.)] 保护防止身份泄露，但未能防止属性泄露。Truta等人 [[31](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR31" \o "Truta TM, Vinay B. Privacy protection: p-sensitive k-anonymity property. In: Proceedings of 22nd international conference on data engineering workshops. 2006. p. 94.)] 提出了 p 敏感匿名，防止身份和属性泄露。其他匿名化方法属于向数据添加噪声、在列中交换单元格以及将 k 记录组替换为单个代表的 k 副本的类。这些方法在匿名化高维数据集时存在一个常见的困难问题 [[32，](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR32" \o "Spruill N. The confidentiality and analytic usefulness of masked business microdata. In: Proceedings on survey research methods. 1983. p. 602–607.)[33](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR33" \o "Chawala S, Dwork C, Sheny FM, Smith A, Wee H. Towards privacy in public databases. In: Proceedings on second theory of cryptography conference. 2005.)] 。

此技术的一个显著好处是，保护大数据部署的成本降低了。当安全数据从安全源迁移到平台时，屏蔽减少了在数据驻留在平台时对该数据应用其他安全控制的需求。

1. 访问控制经过身份验证后，用户可以进入信息系统，但他们的访问仍受访问控制策略的约束，该策略通常基于患者或受信任第三方授权的每个执业者的特权和权利。然后，它是一种强大而灵活的机制，用于向用户授予权限。它提供了复杂的授权控件，以确保用户只能执行他们具有权限的活动，如数据访问、作业提交、群集管理等。

为解决安全和出入控制问题提出了若干解决办法。基于角色的访问控制 （RBAC） [[34](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR34" \o "Science Applications International Corporation (SAIC). Role-based access control (RBAC) Role Engineering Process Version 3.0. 2004.)]和基于属性的访问控制 （ABAC） [[35](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR35" \o "Mohan A, Blough DM. An attribute-based authorization policy framework with dynamic conflict resolution. In: Proceedings of the 9th symposium on identity and trust on the internet. 2010.)， [36](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR36" \o "Hagner M. Security infrastructure and national patent summary. In: Tromso telemedicine and eHealth conference. 2007.)] 是 EHR 最受欢迎的模型。RBAC 和 ABAC 在医疗系统中单独使用时，已显示出一些限制。本文 [[37](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR37" \o "Zhou H, Wen Q. Data security accessing for HDFS based on attribute-group in cloud computing. In: International conference on logistics engineering, management and computer science (LEMCS 2014). 2014.)] 还提出了一种基于 CP-ABE 和对称加密算法（如 AES）的面向云的高效动态访问控制方案。为了满足细粒度访问控制以及安全性和隐私保护的要求，我们建议采用与其他安全技术（如加密和访问控制方法）相结合的技术。

1. 监控和审核安全监控是收集和调查网络事件，以捕捉入侵。审核是指按时间顺序记录医疗保健系统的用户活动，例如维护每次访问和修改数据的日志。这是两个可选的安全指标，用于测量和确保医疗保健系统的安全 [[38](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR38" \o "Linden H, Kalra D, Hasman A, Talmon J. Inter-organization future proof HER systems—a review of the security and privacy related issues. Int J Med Inform. 2009;78:141–60.)] 。

整个网络流量的入侵检测和防护程序相当棘手。为了解决这个问题，通过分析 DNS 流量、IP 流记录、HTTP 流量和蜜罐数据 [[39](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR39" \o "Marchal S, Xiuyan J, State R, Engel T. \“A big data architecture for large scale security monitoring\”, Big Data (BigData Congress), Anchorage, AK. 2014. p. 56–63.)]，开发了一个安全监视体系结构。建议的解决方案包括通过数据关联方案在分布式源中存储和处理数据。在此阶段，已计算三个可能性指标，以确定域名、数据包或流是否为恶意。根据通过此计算获得的分数，警报发生在检测系统中或由预防系统终止的过程。根据开源大数据平台对公司数据电子支付活动的性能分析，Spark 和 Shark 比 Hadoop、Hive 和 Pig [[40](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR40" \o "Duygu ST, Ramazan T, Seref S. A survey on security and privacy issues in big data. In: The 10th international conference for internet technology and secured transactions (ICITST-2015).)] 产生快速稳定的结果。

大数据网络安全系统应快速发现异常，并从异构数据中识别正确的警报。因此，提出了一个大数据安全事件监控系统模型，由四个模块组成：数据收集、集成、分析和解释[[41]。](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR41" \o "Liu L, Lin J. Some special issues of network security monitoring on big data environments. Dependable, Autonomic and Secure Computing (DASC), Chengdu. 2013. p. 10–5.)数据收集包括安全和网络设备日志和事件信息。数据集成过程通过数据筛选和分类执行。在数据分析模块中，确定关联和关联规则以捕获事件。最后，数据解释为知识数据库提供可视化和统计输出，用于决策、预测网络行为和响应事件。

**大医疗保健数据的隐私**

由于出现针对信息系统的高级持续威胁和有针对性的攻击，对患者隐私的侵犯被认为是大数据分析领域日益关注的问题。因此，各组织面临解决这些不同互补和关键问题的挑战。《福布斯》杂志报道的一起事件引起了对病人隐私的警觉[[42]。](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR42" \o "Hill K. How target figured out a teen girl was pregnant before her father did. Forbes, Inc. 2012.)报告提到Target公司向一个父母不知情的少女寄了婴儿护理券。这一事件促使分析和开发人员考虑大数据中的隐私。他们应该能够验证其应用程序是否符合隐私协议，并且无论应用程序和/或隐私法规发生何种变化，敏感信息都保密。

医疗数据隐私是必须认真考虑的重要因素。在下一段，我们引用了一些关于全球隐私保护的法律。

**数据保护法律**

医疗保健组织管理和保护个人信息，并解决其在处理个人数据方面的风险和法律责任，解决越来越多的适用数据保护立法，比以往任何时候都更加重要。不同的国家/地区在数据隐私方面有不同的政策和法律。下表[2](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab2)列出了一些国家/地区的数据保护法规和法律以及显著特征。

表2

**大数据中的隐私保护方法**

这里简要地描述了大数据中保护隐私的传统方法。虽然这些技术传统上用于确保患者的隐私 [[43，](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR43" \o "Big Data security and privacy issues in healthcare—Harsh KupwadePatil, Ravi Seshadri. 2014.)[44，](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR44" \o "Sectorial healthcare strategy 2012–2016-Moroccan healthcare ministry.)[45](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR45" \o "Patil P, Raul R, Shroff R, Maurya M. Big data in healthcare. 2014.)] ， 它们的弊端导致新方法的出现。

1. **去身份化**

取消识别是一种传统方法，通过拒绝任何可以识别患者身份的信息来禁止披露机密信息，无论是要求删除患者的特定标识符的第一种方法，还是通过患者自行验证其删除足够标识符的第二种统计方法。尽管如此，攻击者可能会获得更多的外部信息帮助，以便对大数据进行非标识化。因此，取消标识不足以保护大数据隐私。通过开发有效的隐私保护算法来帮助降低重新识别的风险，可以更可行。引入了k-匿名性[46,47,48]、l-分集[47,49,50]和t-贴近度[46,50]的概念来增强这一传统技术。

* k-匿名在此技术中，k 值越高，重新识别的概率越低。然而，它可能导致数据失真，从而由于k-匿名而造成更大的信息损失。此外，过度的匿名化会使所披露的数据对接收者用处变小，因为某些分析变得不可能，或者可能产生有偏见和错误的结果。在 k 匿名化中，如果使用包含数据的准标识符与其他公开数据链接以识别个人，则会显示作为标识符之一的敏感属性（如疾病）。表[3](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab3)是一个非匿名数据库，由卡萨布兰卡一些虚构医院的病历组成。

表3

此数据中有六个属性和五个记录。对于 k 的某些值，有两种常规技术来实现 k 匿名。第一个是抑制：在此方法中，星号"\*"可以取代属性的某些值。列的部分或全部值可能替换为"\*"。在匿名表[4](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab4)中，将"Name"属性中的每个值和"宗教"属性中的所有值替换为"\*"。

第二种方法是泛化：在此方法中，属性的单个值将替换为更广泛的类别。例如，"出生"字段已通用到年份（例如，属性"Birth"的值"21/11/1972"可能被"1972"年份取代）。邮政编码字段也已通用，以指示更广泛的区域（卡萨布兰卡）。

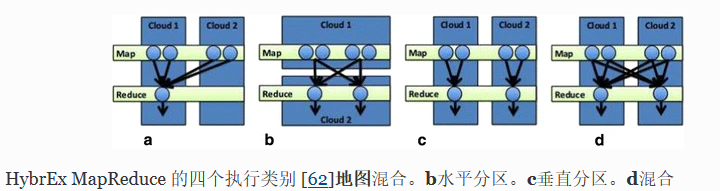
表[4](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab4)对属性"Birth"，"性别"和"ZIP 代码"具有匿名性，因为对于在表的任何行中找到的这些属性的任何混合，始终有不少于两行具有这些确切属性的行。对于具有 k 匿名的数据集，每个"准标识符"元组都至少出现在 k 记录中。k-匿名数据仍然可以对攻击（如未排序的匹配攻击、时态攻击和互补释放攻击）束手无策 [[50，](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR50" \o "Samarati P, Sweeney L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical Report SRI-CSL-98-04, SRI Computer Science Laboratory. 1998.) [51](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR51" \o "Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness. 2002;10(5):557–70.)] 。从好的方面看，呈现私有记录关系（k-匿名）的复杂性，同时最大限度地减少未发布的信息量，同时确保个人匿名至一组大小 k，并保留最小数量的信息以实现此隐私级别，此优化问题是 NP-hard [[52](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR52" \o "Meyerson A, Williams R. On the complexity of optimal k-anonymity. In: Proc. of the ACM Symp. on principles of database systems. 2004.)] 。已提出各种措施来量化匿名造成的信息损失，但它们没有反映数据的实际有用性[[53，54]。](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR53" \o "Iyenger V. Transforming data to satisfy privacy constraints. In: Proceedings of the ACM SIGKDD. 2002;279–88.) 因此，我们朝着数据匿名化的L-多样性策略迈进。

* L-多样性这是一种基于群的匿名化形式，通过减少数据表示的粒度来保护数据集的隐私。此模型（差异、熵、递归）[[46、](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR46" \o "Li N, et al. t-Closeness: privacy beyond k-anonymity and L-diversity. In: Data engineering (ICDE) IEEE 23rd international conference. 2007.) [47](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR47" \o )、 [51](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR51" \o "Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness. 2002;10(5):557–70.)]k 匿名性，它使用包括概括和抑制在内的方法，以任何给定的记录映射到数据中至少 k 个不同的记录的方式降低数据表示的粒度。l-分集模型处理 k 匿名模型中的一些弱点，其中保护身份到 k-个人级别并不等于保护被概括或抑制的相应敏感值。此方法的问题在于它取决于敏感属性的范围。如果想要使数据 L 多样化，尽管敏感属性没有不同值，则要插入虚构的数据。这种虚构的数据将提高安全性，但可能会导致分析中的问题。因此，L-分集法也是受偏颇和相似性攻击的一个对象，[即[51](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR51" \o "Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness. 2002;10(5):557–70.)]，因此不能阻止属性泄露。
* T-接近性是基于匿名化的l-多样性群体的进一步改进。t-接近度模型（相等/分层距离）[[46](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR46" \o "Li N, et al. t-Closeness: privacy beyond k-anonymity and L-diversity. In: Data engineering (ICDE) IEEE 23rd international conference. 2007.)， [50](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR50" \o "Samarati P, Sweeney L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical Report SRI-CSL-98-04, SRI Computer Science Laboratory. 1998.)]通过明确处理属性的值来扩展 l-分集模型，同时考虑到该属性的数据值分布。这种技术的主要优点是它拦截了属性泄露，它的问题是，随着数据的大小和种类的增加，重新识别的可能性也会增加。

1. **海布雷克斯**

混合执行模型 [[55](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR55" \o "Priyank J, Manasi G, Nilay K. Big data privacy: a technological perspective and review. J Big Data. 2016;3:25.)] 是云计算中保密和隐私的模型。它仅将公共云用于组织的非敏感数据归类为公共的计算，即当组织声明使用公共云导出数据并对其执行计算时没有隐私和保密风险，而对于组织的敏感私有数据和计算，模型将执行其私有云。此外，当应用程序需要访问私有数据和公共数据时，应用程序本身也会被分区并在私有云和公共云中运行。它在作业执行之前考虑数据敏感度，并提供安全性的集成。

HybrEx MapReduce 支持使用公共云和私有云的新型应用程序的四个类别，如图[2](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Fig2)所示。

图2

1. 地图混合 （1a）映射阶段在公共云和私有云中执行，而减少阶段仅在其中一个云中执行。
2. 垂直分区 （1b）在公共云中使用公共数据作为输入，在其中随机排列中间数据，并将结果存储在公共云中，从而在公共云中执行映射和减少任务。在私有云中使用私有数据完成相同的工作。作业是单独处理的。
3. 水平分区 （1c）映射阶段仅在公共云中执行，而减少阶段在私有云中执行。
4. 混合 （1d）在公共云和私有云上执行映射阶段和减少阶段。云之间的数据传输也是可能的。
5. HybridEx 的问题是，它不处理在映射阶段在公共云和私有云中生成的密钥，并且它只处理作为对手的云 [[55](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR55" \o "Priyank J, Manasi G, Nilay K. Big data privacy: a technological perspective and review. J Big Data. 2016;3:25.)] 。
6. **基于身份的匿名化**

它是一种信息清理，其意图是隐私保护。它是从数据集中加密或删除个人身份信息的过程，以便数据描述的人员保持匿名。此技术的主要困难涉及将匿名化、隐私保护和大数据技术 [[56](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR56" \o "Sedayao J, Bhardwaj R. Making big data, privacy, and anonymization work together in the enterprise: experiences and issues. In: Big data congress. 2014.)] 相结合，在保护身份的同时分析使用情况数据。

英特尔人为因素工程团队需要使用网页访问日志和大数据工具保护英特尔员工的隐私，以提高英特尔大量使用的内部 Web 门户的便利性。他们被要求从门户的使用日志存储库中删除个人识别信息 （PII），但方式不会影响大数据工具执行分析或重新识别日志条目以调查异常情况的能力行为。

为了满足云存储 [[57](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR57" \o "Yong Yu, et al. Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Gen Comput Syst. 2016;62:85–91.)] 的巨大优势，英特尔创建了一个用于匿名化的开放式体系结构 [[56](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR56" \o "Sedayao J, Bhardwaj R. Making big data, privacy, and anonymization work together in the enterprise: experiences and issues. In: Big data congress. 2014.)]，允许使用各种工具来取消识别和重新识别 Web 日志记录。在实现体系结构过程中，企业数据具有不同于匿名文献中的标准示例 [[58](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR58" \o )] 的属性。英特尔还发现，尽管屏蔽了用户名和 IP 地址等明显的个人识别信息，但匿名数据对相关攻击毫无防备。在探索了纠正这些漏洞的权衡后，他们发现用户代理信息与单个用户密切相关。这是企业中匿名实现的案例研究，描述了使用大数据技术分析的企业数据中使用匿名保护隐私时遇到的要求、实施和经验。这种对匿名质量的调查使用了基于 k 匿名的指标。英特尔使用 Hadoop 分析匿名数据，并为人为因素分析师获取有价值的结果 [[59，](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR59" \o ) [60](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR60" \o )]同时，它了解到匿名化需要不仅仅是掩盖或概括某些字段，还需要仔细分析匿名数据集，以确定它们是否容易受到攻击。

**大数据隐私中最近使用的方法摘要**

在本文中，我们讨论了大数据中的安全和隐私挑战，讨论了一些现有的实现医疗保健组织可能非常有益的实现安全和隐私的方法和技术。在本节中，我们重点引用了不同论文中提出的一些方法和技术，重点是它们的重点和局限性（表[5）。](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab5)

例如，在 Hadoop 中建议了隐私保留数据挖掘技术。论文 [[67](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR67" \o "Lu R, Zhu H, Liu X, Liu JK, Shao J. Toward efficient and privacy-preserving computing in big data era. IEEE Netw. 2014;28:46–50.)] 还介绍了一种高效且隐私保护的后因相似性计算协议，并讨论了现有方法"差异隐私"如何适用于大数据。此外，论文[[69](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR69" \o "Zhang X, Yang T, Liu C, Chen J. A scalable two-phase top-down specialization approach for data anonymization using systems, in MapReduce on cloud. IEEE Trans Parallel Distrib. 2014;25(2):363–73.)] 建议采用一种可扩展的方法来匿名化大规模数据集。论文 [[70](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR70" \o "Mehmood A, Natgunanathan I, Xiang Y, Hua G, Guo S. Protection of big data privacy. In: IEEE translations and content mining are permitted for academic research. 2016.)] 提出了处理大数据应用程序的各种隐私问题，而论文 [[71](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR71" \o "Mohammadian E, Noferesti M, Jalili R. FAST: fast anonymization of big data streams. In: ACM proceedings of the 2014 international conference on big data science and computing, article 1. 2014.)] 提出了一种匿名算法，以加快大数据流的匿名化。此外，论文 [[72](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR72" \o "Xu K, Yue H, Guo Y, Fang Y. Privacy-preserving machine learning algorithms for big data systems. In: IEEE 35th international conference on distributed systems. 2015.)] 提出了一种新的框架，以实现保护隐私的机器学习和纸张 [[73](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR73" \o "Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing. Inf Sci. 2014;258:371–86.)] 建议的方法来提供数据机密性和安全数据共享。所有这些技术和方法都显示出一些局限性。

与以前的模型相比，这些增加的复杂性和限制使新模型更难解释，其可靠性也不易评估。

**结论**

虽然大数据在医疗保健领域的潜在机会是无限的（例如，推动健康研究、知识发现、临床护理和个人健康管理），但有几个障碍阻碍其真正的潜力，包括技术挑战、隐私和安全问题以及技术人才。大数据安全和隐私被认为是该领域研究人员的巨大障碍。

在本文中，我们简要地讨论了一些成功的相关工作在世界各地。我们还介绍了大数据生命周期每个阶段的隐私和安全问题，以及大医疗保健数据隐私和安全背景下现有技术的优点和缺陷。

我们主要回顾了最近在医疗保健领域使用的隐私保护方法，并讨论了加密和匿名方法如何用于医疗保健数据保护，并介绍了这些方法的局限性。此外，还有更多的技术包括隐藏针在干草堆 [[61](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR61" \o "Jung K, Park S, Park S. Hiding a needle in a haystack: privacy preserving Apriori algorithm in MapReduce framework PSBD’14, Shanghai. 2014. p. 11–7.)]， 基于属性的加密访问控制， 同构加密， 存储路径加密等.然而，问题总是强加于人。

在此背景下，作为我们未来的发展方向，在大型医疗保健数据时代实现隐私和安全的有效解决方案。同样，隐私方法也需要加强。

同时，随着物联网的快速发展，数量越大，质量越低。因此，由于研究人员获得适当的结果，隐私保护算法不应对数据质量产生更大的影响。更进一步，我们将尝试通过模拟不同方法最终支持决策和规划策略来解决安全与隐私模型的调和问题。

**原文：**

**Big healthcare data: preserving security and privacy**

[Journal of Big Data](https://link.springer.xilesou.top/journal/40537) volume 5, Article number: 1 (2018)

**Abstract**

Big data has fundamentally changed the way organizations manage, analyze and leverage data in any industry. One of the most promising fields where big data can be applied to make a change is healthcare. Big healthcare data has considerable potential to improve patient outcomes, predict outbreaks of epidemics, gain valuable insights, avoid preventable diseases, reduce the cost of healthcare delivery and improve the quality of life in general. However, deciding on the allowable uses of data while preserving security and patient’s right to privacy is a difficult task. Big data, no matter how useful for the advancement of medical science and vital to the success of all healthcare organizations, can only be used if security and privacy issues are addressed. To ensure a secure and trustworthy big data environment, it is essential to identify the limitations of existing solutions and envision directions for future research. In this paper, we have surveyed the state-of-the-art security and privacy challenges in big data as applied to healthcare industry, assessed how security and privacy issues occur in case of big healthcare data and discussed ways in which they may be addressed. We mainly focused on the recently proposed methods based on anonymization and encryption, compared their strengths and limitations, and envisioned future research directions.

**Introduction**

Change is the new norm for the global healthcare sector. In fact, digitization of health and patient data is undergoing a dramatic and fundamental shift in the clinical, operating and business models and generally in the world of economy for the foreseeable future. This shift is being spurred by aging populations and lifestyle changes; the proliferation of software applications and mobile devices; innovative treatments; heightened focus on care quality and value; and evidence-based medicine as opposed to subjective clinical decisions—all of which are leading to offer significant opportunities for supporting clinical decision, improving healthcare delivery, management and policy making, surveilling disease, monitoring adverse events, and optimizing treatment for diseases affecting multiple organ systems [[1](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR1" \o "Burghard C. Big data and analytics key to accountable care success. Framingham: IDC Health Insights; 2012.), [2](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR2" \o "Fernandes L, O’Connor M, Weaver V. Big data, bigger outcomes. J AHIMA. 2012;83:38–42.)].

As noted above, big data analytics in healthcare carries many benefits, promises and presents great potential for transforming healthcare, yet it raises manifold barriers and challenges. Indeed, the concerns over the big healthcare data security and privacy are increased year-by-year. Additionally, healthcare organizations found that a reactive, bottom-up, technology-centric approach to determining security and privacy requirements is not adequate to protect the organization and its patients [[3](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR3" \o "David Houlding, MSc, CISSP. Health Information at Risk: Successful Strategies for Healthcare Security and Privacy. Healthcare IT Program Of ce Intel Corporation, white paper. 2011.)].

Motivated thus, new information systems and approaches are needed to prevent breaches of sensitive information and other types of security incidents so as to make effective use of the big healthcare data.

In this paper, we discuss some interesting related works and present risks to the big health data security as well as some newer technologies to redress these risks. Then, we focus on the big data privacy issue in healthcare, by mentioning various laws and regulations established by different regulatory bodies and pointing out some feasible techniques used to ensure the patient’s privacy. Thereafter, we provide some proposed techniques and approaches that were reported in the literature to deal with security and privacy risks in healthcare while identifying their limitations. Lastly, we offer conclusions and highlight the future directions.

### **Successful related works**

Seamless integration of greatly diverse big healthcare data technologies can not only enable us to gain deeper insights into the clinical and organizational processes but also facilitate faster and safer throughput of patients and create greater efficiencies and help improve patient flow, safety, quality of care and the overall patient experience no matter how costly it is.

Such was the case with South Tyneside NHS Foundation Trust, a provider of acute and community health services in northeast England that understands the importance of providing high quality, safe and compassionate care for the patients at all times, but needs a better understanding of how its hospitals operate to improve resource allocation and wait times and to ensure that any issues are identified early and acted upon [[4](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR4" \o "South Tyneside NHS Foundation Trust. Harnessing analytics for strategic planning, operational decision making and end-to-end improvements in patient care. IBM Smarter Planet brief. 2013.)].

Another example is the UNC Health Care (UNCHC), which is a non-profit integrated healthcare system in North Carolina that has implemented a new system allowing clinicians to rapidly access and analyze unstructured patient data using natural-language processing. In fact, UNCHC has accessed and analyzed huge quantities of unstructured content contained in patient medical records to extract insights and predictors of readmission risk for timely intervention, providing safer care for high-risk patients and reducing re-admissions [[5](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR5" \o "UNC Health Care relies on analytics to better manage medical data and improve patient care. IBM Press release. 2013.)].

Moreover in the United States, the Indiana Health Information Exchange, which is a non-profit organization, provides a secure and robust technology network of health information linking more than 90 hospitals, community health clinics, rehabilitation centers and other healthcare providers in Indiana. It allows medical information to follow the patient hosted in one doctor office or only in a hospital system [[6](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR6" \o )].

One more example is Kaiser Permanente medical network based in California. It has more than 9 million members, estimated to manage large volumes of data ranging from 26.5 Petabytes to 44 Petabytes. [[7](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR7" \o "Transforming healthcare through big data, strategies for leveraging big data in the healthcare industry. Institute for Health. 2013.)].

Big data analytics is used also in Canada, e.g. the infant hospital of Toronto. This hospital succeeded to improve the outcomes for newborns prone to serious hospital infections. Another example is the Artemis project, which is a newborns monitoring platform designed mercy to a collaboration between IBM and the Institute of Technology of Ontario. It supported the acquisition and the storage of patients’ physiological data and clinical information system data for the objective of online and real time analysis, retrospective analysis, and data mining [[8](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR8" \o )].

In Europe and exactly in Italy, the Italian medicines agency collects and analyzes a large amount of clinical data concerning expensive new medicines as part of a national profitability program. Based on the results, it may reassess the medicines prices and market access terms [[9](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR9" \o "Groves P, Kayyali B, Knott D, Kuiken SV. The big data revolution in healthcare, accelerating value and innovation. 2013.)].

In the domain of mHealth, the World Health Organization has launched the project “Be Healthy Be mobile” in Senegal and under the mDiabetes initiative it supports countries to set up large-scale projects that use mobile technology, in particular text messaging and apps, to control, prevent and manage non-communicable diseases such as diabetes, cancer and heart disease [[10](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR10" \o "WHO. Mobile phones help people with diabetes to manage fasting and feasting during Ramadan. Features. 2014.)]. mDiabetes is the first initiative to take advantage of the widespread mobile technology to reach millions of Senegalese people with health information and expand access to expertise and care. Launched in 2013, in Costa Rica that has been officially selected as the first country, the initiative is working on an mCessation for tobacco program for smoking prevention and helping smokers quit, an mCervical cancer program in Zambia and has plans to roll out mHypertension and mWellness programs in other countries.

After Europe, Canada, Australia, Russia, and Latin America, Sophia Genetics [[11](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR11" \o "Sophia Genetics. «Product & Technology Overview» 2014.)], global leader in data-driven medicine, announced at the recent 2017 Annual Meeting of the American College of Medical Genetics and Genomics (ACMG) that its artificial intelligence has been adopted by African hospitals to advance patient care across the continent.

In Morocco for instance, PharmaProcess in Casablanca, ImmCell, The Al Azhar Oncology Center and The Riad Biology Center in Rabat are some medical institutions at the forefront of innovation that have started integrating Sophia to speed and analyze genomic data to identify disease-causing mutations in patients’ genomic profiles, and decide on the most effective care. As new users of SOPHIA, they become part of a larger network of 260 hospitals in 46 countries that share clinical insights across patient cases and patient populations, which feeds a knowledge-base of biomedical findings to accelerate diagnostics and care [[12](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR12" \o )].

While the automations have led to improve patient care workflow and reduce costs, it is also rising healthcare data to increase probability of security and privacy breaches. In 2016, CynergisTek has released the Redspin’s 7th annual breach report: Protected Health Information (PHI) [[13](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR13" \o "CynergisTek, Redspin. «BREACH REPORT 2016: Protected Health Information (PHI)» 2017.)] in which it has reported that hacking attacks on healthcare providers were increased 320% in 2016, and that 81% of records breached in 2016 resulted from hacking attacks specifically. Additionally, ransomware, defined as a type of malware that encrypts data and holds it hostage until a ransom demand is met, has identified as the most prominent threat to hospitals. Additional findings of this report include:

* 325 large breaches of PHI, compromising 16,612,985 individual patient records.
* 3,620,000 breached patient records in the year’s single largest incident.
* 40% of large breach incidents involved unauthorized access/disclosure.

These findings point to a pressing need for providers to take a much more proactive and comprehensive approach to protecting their information assets and combating the growing threat that cyber attacks present to healthcare.

Several prosperous initiatives have appeared to help the healthcare industry continually improve its ability to protect patient information.

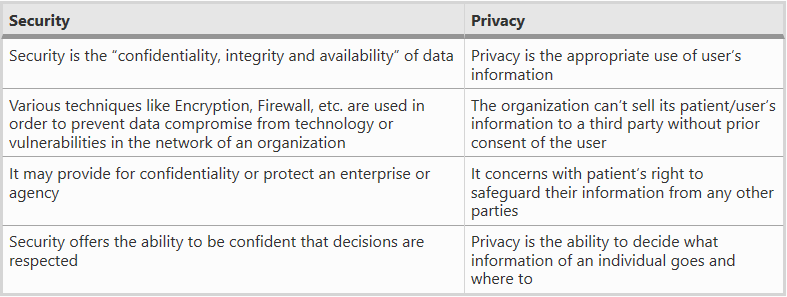
In January 2014, for example, the White House, led by President Obama’s Counselor John Podesta, undertook a 90-day review of big data and privacy. The review brought concrete recommendations to maximize benefits and minimize risks of big data [[14](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR14" \o "Podesta J, et al. Big data: seizing opportunities, preserving values. Executive Office of the President. 2014;1:2013.), [15](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR15" \o "House W. Big data and privacy: a technological perspective. Washington: Executive Office of the President, President’s Council of Advisors on Science and Technology; 2014.)], namely:

* Policy attention should focus more on the actual uses of big data and less on its collection and analysis. Such existing policies are unlikely to yield effective strategies for improving privacy, or to be scalable over time.
* Policy concerning privacy protection should be addressing the purpose rather than prescribing the mechanism.
* Research is needed in the technologies that help to protect privacy, in the social mechanisms that influence privacy preserving behavior, and in the legal options that are robust to changes in technology and create appropriate balance among economic opportunity, national priorities, and privacy protection.
* Increased education and training opportunities concerning privacy protection, including career paths for professionals. Programs that provide education leading to privacy expertise are essential and need encouragement.
* Privacy protections should be extended to non-US citizens as privacy is a worldwide value that should be reflected in how the federal government handles personally identifiable information from non-US citizens [[16](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR16" \o "House W. FACT SHEET: big data and privacy working group review. 2014.)].

The OECD Health Care Quality Indicators (HCQI) project is responsible for a plan in 2013/2014 to develop tools to assist countries in balancing data privacy risks and risks from not developing and using health data. This plan includes developing a risk categorization of different types and uses of data and the promising practices that countries can deploy to reduce risks that directly affect everyone’s daily life and enable data use [[17](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR17" \o "OECD. Data-driven healthcare innovation, management and policy, DELSA/HEA(2013)13. Paris: OECD; 2013.)].

### **Privacy and security concerns in big data**

Security and privacy in big data are important issues. Privacy is often defined as having the ability to protect sensitive information about personally identifiable health care information. It focuses on the use and governance of individual’s personal data like making policies and establishing authorization requirements to ensure that patients’ personal information is being collected, shared and utilized in right ways. While security is typically defined as the protection against unauthorized access, with some including explicit mention of integrity and availability. It focuses on protecting data from pernicious attacks and stealing data for profit. Although security is vital for protecting data but it’s insufficient for addressing privacy. Table [1](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab1) focuses on additional difference between security and privacy.



### **Security of big healthcare data**

While healthcare organizations store, maintain and transmit huge amounts of data to support the delivery of efficient and proper care, the downsides are the lack of technical support and minimal security. Complicating matters, the healthcare industry continues to be one of the most susceptible to publicly disclosed data breaches. In fact, attackers can use data mining methods and procedures to find out sensitive data and release it to the public and thus data breach happens. Whereas implementing security measures remains a complex process, the stakes are continually raised as the ways to defeat security controls become more sophisticated.

Accordingly, it is critical that organizations implement healthcare data security solutions that will protect important assets while also satisfying healthcare compliance mandates.

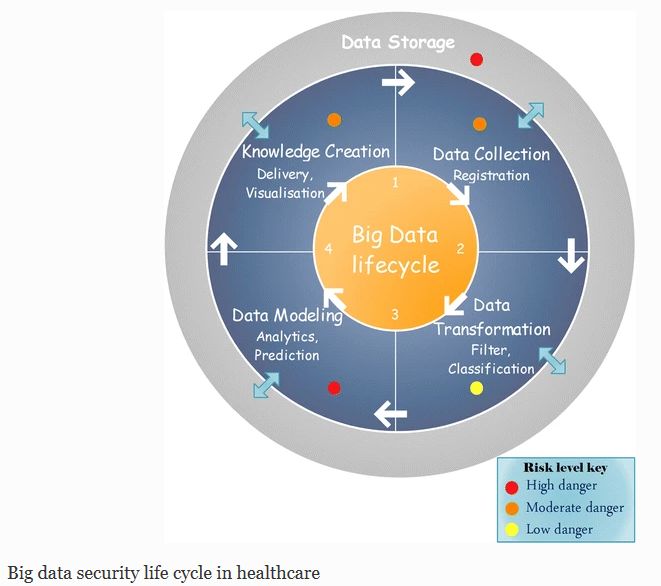
**A. Big data security lifecycle**

In terms of security and privacy perspective, Kim et al. [[18](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR18" \o )] argue that security in big data refers to three matters: data security, access control, and information security. In this regards, healthcare organizations must implement security measures and approaches to protect their big data, associated hardware and software, and both clinical and administrative information from internal and external risks. At a project’s inception, the data lifecycle must be established to ensure that appropriate decisions are made about retention, cost effectiveness, reuse and auditing of historical or new data [[19](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR19" \o "\“Data-driven healthcare organizations use big data analytics for big gains\” IBM white paper February. 2013.)].

Yazan et al. [[20](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR20" \o "Yazan A, Yong W, Raj Kumar N. Big data life cycle: threats and security model. In: 21st Americas conference on information systems. 2015.)] suggested a big data security lifecycle model extended from Xu et al. [[21](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR21" \o )]. This model is designed to address the phases of the big data lifecycle and correlate threats and attacks that face big data environment within these phases, while [[21](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR21" \o )] address big data lifecycle from user role perspective: data provider, data collector, data miner, and decision maker. The model proposed in [[20](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR20" \o "Yazan A, Yong W, Raj Kumar N. Big data life cycle: threats and security model. In: 21st Americas conference on information systems. 2015.)] comprised of four interconnecting phases: data collection phase, data storage phase, data processing and analysis, and knowledge creation.

Furthermore, CCW (The Chronic Conditions Data Warehouse) follows a formal information security lifecycle model, which consists of four core phases that serve to identify, assess, protect and monitor against patient data security threats. This lifecycle model is continually being improved with emphasis on constant attention and continual monitoring [[21](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR21" \o )].

In this paper, we suggest a model that combines the phases presented in [[20](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR20" \o "Yazan A, Yong W, Raj Kumar N. Big data life cycle: threats and security model. In: 21st Americas conference on information systems. 2015.)] and phases mentioned in [[21](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR21" \o )], in order to provide encompass policies and mechanisms that ensure addressing threats and attacks in each step of big data life cycle. Figure [1](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Fig1) presents the main elements in big data lifecycle in healthcare.



* Data collection phase This is the obvious first step. It involves collecting data from different sources in various formats. From a security perspective, securing big health data technology is a necessary requirement from the first phase of the lifecycle. Therefore, it is important to gather data from trusted sources, preserve patient privacy (there must be no attempt to identify the individual patients in the database) and make sure that this phase is secured and protected. Indeed, some mature security measures must be used to ensure that all data and information systems are protected from unauthorized access, disclosure, modification, duplication, diversion, destruction, loss, misuse or theft.
* Data transformation phase Once the data is available, the first step is to filter and classify the data based on their structure and do any necessary transformations in order to perform meaningful analysis. More broadly, data filtering, enrichment and transformation are needed to improve the quality of the data ahead of analytics or modeling phase and remove or appropriately deal with noise, outliers, missing values, duplicate data instances, etc. On the other side, the collected data may contain sensitive information, which makes extremely important to take sufficient precautions during data transformation and storing. In order to guarantee the safety of the collected data, the data should remain isolated and protected by maintaining access-level security and access control (utilizing an extensive list of directories and databases as a central repository for user credentials, application logon templates, password policies and client settings) [[22](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR22" \o )], and defining some security measures like data anonymization approach, permutation, and data partitioning.
* Data modeling phase Once the data has been collected, transformed and stored in secured storage solutions, the data processing analysis is performed to generate useful knowledge. In this phase, supervised data mining techniques such as clustering, classification, and association can be employed for feature selection and predictive modeling. Further, there also exist several ensembles of learning techniques that improve accuracy and robustness of the final model. On the other side, it is crucial to provide secure processing environment. In fact, the focus of data miners in this phase is to use powerful data mining algorithms that can extract sensitive data. Therefore, the process of data mining and the network components in general, must be configured and protected against data mining based attacks and any security breach that may happen, as well as make sure that only authorized staff work in this phase. This process helps eliminate some vulnerabilities and mitigates others to a lower risk level.
* Knowledge creation phase Finally, the modeling phase comes up with new information and valued knowledges to be used by decision makers. These created knowledges are considered sensitive data, especially in a competitive environment. Indeed, healthcare organizations aware of their sensitive data (e.g. patient personal data) not to be publicly released. Accordingly, security compliance and verification are a primary objective in this phase.
* At all stages of big data lifecycle, it requires data storage, data integrity and data access control.

**B. Technologies in use**

Various technologies are in use to ensure security and privacy of big healthcare data. Most widely used technologies are:

1) Authentication Authentication is the act of establishing or confirming claims made by or about the subject are true and authentic. It serves vital functions within any organization: securing access to corporate networks, protecting the identities of users, and ensuring that the user is really who he is pretending to be.

The information authentication can pose special problems, especially man-in-the-middle (MITM) attacks. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For instance [[23](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR23" \o "Zhang R, Liu L. Security models and requirements for healthcare application clouds. In: IEEE 3rd international conference on cloud computing. 2010.)], transport layer security (TLS) and its predecessor, secure sockets layer (SSL), are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the transport layer end-to-end. Several versions of the protocols are in widespread use in applications like web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP). One can use SSL or TLS to authenticate the server using a mutually trusted certification authority. Hashing techniques like SHA-256 [[24](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR24" \o "Shafer J, Rixner S, Cox AL. The hadoop distributed filesystem: balancing portability and performance. In: Proceedings of 2010 IEEE international symposium on performance analysis of systems & software (ISPASS), March 2010, White Plain, NY. p. 122–33.)] and Kerberos mechanism based on Ticket Granting Ticket or Service Ticket can be also implemented to achieve authentication. Additionally, Bull Eye algorithm can be used for monitoring all sensitive information in 360°. This algorithm has been used to make sure data security and manage relations between original data and replicated data. It is also allowed only to an authorized person to read or write critical data. Paper [[25](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR25" \o "Yang C, Lin W, Liu M. A novel triple encryption scheme for hadoop-based cloud data security. In: Emerging intelligent data and web technologies (EIDWT), 2013 fourth international conference on. 2013. p. 437–42.)] proposes a novel and simple authentication model using one time pad algorithm. It provides removing the communication of passwords between the servers. In a healthcare system, both healthcare information offered by providers and identities of consumers should be verified at the entry of every access.

2) Encryption Data encryption is an efficient means of preventing unauthorized access of sensitive data. Its solutions protect and maintain ownership of data throughout its lifecycle—from the data center to the endpoint (including mobile devices used by physicians, clinicians, and administrators) and into the cloud. Encryption is useful to avoid exposure to breaches such as packet sniffing and theft of storage devices.

Healthcare organizations or providers must ensure that encryption scheme is efficient, easy to use by both patients and healthcare professionals, and easily extensible to include new electronic health records. Furthermore, the number of keys hold by each party should be minimized.

Although various encryption algorithms have been developed and deployed relatively well (RSA, Rijndael, AES and RC6 [[24](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR24" \o "Shafer J, Rixner S, Cox AL. The hadoop distributed filesystem: balancing portability and performance. In: Proceedings of 2010 IEEE international symposium on performance analysis of systems & software (ISPASS), March 2010, White Plain, NY. p. 122–33.), [26](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR26" \o "Federal Information Processing Standards Publication 197. Specification for the advanced encryption standards (AES). 2001.), [27](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR27" \o "Somu N, Gangaa A, Sriram VS. Authentication service in hadoop using one time pad. Indian J Sci Technol. 2014;7:56–62.)], DES, 3DES, RC4 [[28](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR28" \o "Fluhrer S, Mantin I, Shamir A. Weakness in the key scheduling algorithm of RC4. In: 8th annual international workshop on selected areas in cryptography, London: Springer-Verlag. 2001.)], IDEA, Blowfish …), the proper selection of suitable encryption algorithms to enforce secure storage remains a difficult problem.

3) Data masking Masking replaces sensitive data elements with an unidentifiable value. It is not truly an encryption technique so the original value cannot be returned from the masked value. It uses a strategy of de-identifying data sets or masking personal identifiers such as name, social security number and suppressing or generalizing quasi-identifiers like date-of-birth and zip-codes. Thus, data masking is one of the most popular approach to live data anonymization. k-anonymity first proposed by Swaney and Samrati [[29](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR29" \o "Sweeney L. Achieving k-anonymity privacy protection using generalization and suppression. Int J Uncertain Fuzziness Knowl Based Syst. 2002;10:571–88.), [30](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR30" \o "Samrati P. Protecting respondents identities in microdata release. IEEE Trans Knowl Data Eng. 2001;13:1010–27.)] protects against identity disclosure but failed to protect against attribute disclosure. Truta et al. [[31](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR31" \o "Truta TM, Vinay B. Privacy protection: p-sensitive k-anonymity property. In: Proceedings of 22nd international conference on data engineering workshops. 2006. p. 94.)] have presented p-sensitive anonymity that protects against both identity and attribute disclosure. Other anonymization methods fall into the classes of adding noise to the data, swapping cells within columns and replacing groups of k records with k copies of a single representative. These methods have a common problem of difficulty in anonymizing high dimensional data sets [[32](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR32" \o "Spruill N. The confidentiality and analytic usefulness of masked business microdata. In: Proceedings on survey research methods. 1983. p. 602–607.), [33](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR33" \o "Chawala S, Dwork C, Sheny FM, Smith A, Wee H. Towards privacy in public databases. In: Proceedings on second theory of cryptography conference. 2005.)].

A significant benefit of this technique is that the cost of securing a big data deployment is reduced. As secure data is migrated from a secure source into the platform, masking reduces the need for applying additional security controls on that data while it resides in the platform.

4) Access control Once authenticated, the users can enter an information system but their access will still be governed by an access control policy which is typically based on privileges and rights of each practitioner authorized by patient or a trusted third party. It is then, a powerful and flexible mechanism to grant permissions for users. It provides sophisticated authorization controls to ensure that users can perform only the activities for which they have permissions, such as data access, job submission, cluster administration, etc.

A number of solutions have been proposed to address the security and access control concerns. Role-based access control (RBAC) [[34](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR34" \o "Science Applications International Corporation (SAIC). Role-based access control (RBAC) Role Engineering Process Version 3.0. 2004.)] and attribute-based access control (ABAC) [[35](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR35" \o "Mohan A, Blough DM. An attribute-based authorization policy framework with dynamic conflict resolution. In: Proceedings of the 9th symposium on identity and trust on the internet. 2010.), [36](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR36" \o "Hagner M. Security infrastructure and national patent summary. In: Tromso telemedicine and eHealth conference. 2007.)] are the most popular models for EHR. RBAC and ABAC have shown some limitations when they are used alone in medical system. Paper [[37](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR37" \o "Zhou H, Wen Q. Data security accessing for HDFS based on attribute-group in cloud computing. In: International conference on logistics engineering, management and computer science (LEMCS 2014). 2014.)] proposes also a cloud-oriented storage efficient dynamic access control scheme ciphertext based on the CP-ABE and a symmetric encryption algorithm (such as AES). To satisfy requirements of fine-grained access control yet security and privacy preserving, we suggest adopting technologies in conjunction with other security techniques, e.g. encryption, and access control methods.

5) Monitoring and auditing Security monitoring is gathering and investigating network events to catch the intrusions. Audit means recording user activities of the healthcare system in chronological order, such as maintaining a log of every access to and modification of data. These are two optional security metrics to measure and ensure the safety of a healthcare system [[38](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR38" \o "Linden H, Kalra D, Hasman A, Talmon J. Inter-organization future proof HER systems—a review of the security and privacy related issues. Int J Med Inform. 2009;78:141–60.)].

Intrusion detection and prevention procedures on the whole network traffic is quite tricky. To address this problem, a security monitoring architecture has been developed via analyzing DNS traffic, IP flow records, HTTP traffic and honeypot data [[39](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR39" \o "Marchal S, Xiuyan J, State R, Engel T. \“A big data architecture for large scale security monitoring\”, Big Data (BigData Congress), Anchorage, AK. 2014. p. 56–63.)]. The suggested solution includes storing and processing data in distributed sources through data correlation schemes. At this stage, three likelihood metrics have been calculated to identify whether domain name, packet or flow is malicious. Depending on the score obtained through this calculation, an alert occurs in detection system or process terminate by prevention system. According to performance analysis with open source big data platforms on electronic payment activities of a company data, Spark and Shark produce fast and steady results than Hadoop, Hive and Pig [[40](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR40" \o "Duygu ST, Ramazan T, Seref S. A survey on security and privacy issues in big data. In: The 10th international conference for internet technology and secured transactions (ICITST-2015).)].

Big data network security systems should be find abnormalities quickly and identify correct alerts from heterogeneous data. Therefore, a big data security event monitoring system model has been proposed which consists of four modules: data collection, integration, analysis, and interpretation [[41](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR41" \o "Liu L, Lin J. Some special issues of network security monitoring on big data environments. Dependable, Autonomic and Secure Computing (DASC), Chengdu. 2013. p. 10–5.)]. Data collection includes security and network devices logs and event information. Data integration process is performed by data filtering and classifying. In data analysis module, correlations and association rules are determined to catch events. Finally, data interpretation provides visual and statistical outputs to knowledge database that makes decisions, predicts network behavior and responses events.

### **Privacy of big healthcare data**

The invasion of patient privacy is considered as a growing concern in the domain of big data analytics due to the emergence of advanced persistent threats and targeted attacks against information systems. As a result, organizations are in challenge to address these different complementary and critical issues. An incident reported in the Forbes magazine raises an alarm over patient privacy [[42](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR42" \o "Hill K. How target figured out a teen girl was pregnant before her father did. Forbes, Inc. 2012.)]. In the report, it mentioned that Target Corporation sent baby care coupons to a teen-age girl unbeknown to her parents. This incident impels analytics and developers to consider privacy in big data. They should be able to verify that their applications conform to privacy agreements and that sensitive information is kept private regardless of changes in applications and/or privacy regulations.

Privacy of medical data is then an important factor which must be seriously considered. We cite in the next paragraph some of laws on the privacy protection worldwide.

### **Data protection laws**

More than ever it is crucial that healthcare organizations manage and safeguard personal information and address their risks and legal responsibilities in relation to processing personal data, to address the growing thicket of applicable data protection legislation. Different countries have different policies and laws for data privacy. Data protection regulations and laws in some of the countries along with salient features are listed in Table [2](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab2) below.



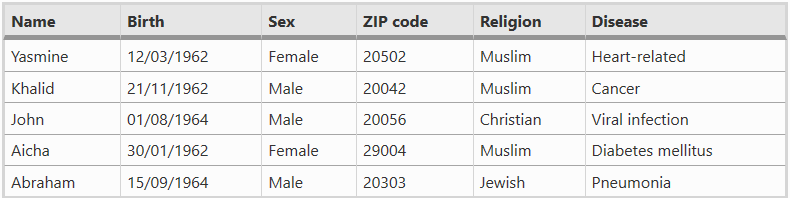
### **Privacy preserving methods in big data**

Few traditional methods for privacy preserving in big data are described in brief here. Although these techniques are used traditionally to ensure the patient’s privacy [[43](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7" \l "ref-CR43" \o "Big Data security and privacy issues in healthcare—Harsh KupwadePatil, Ravi Seshadri. 2014.),[44](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7" \l "ref-CR44" \o "Sectorial healthcare strategy 2012–2016-Moroccan healthcare ministry.),[45](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR45" \o "Patil P, Raul R, Shroff R, Maurya M. Big data in healthcare. 2014.)], their demerits led to the advent of newer methods.

#### **A. De-identification**

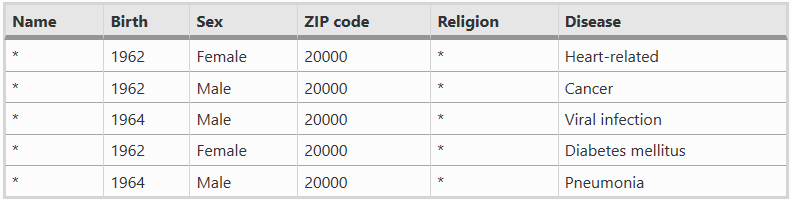
De-identification is a traditional method to prohibit the disclosure of confidential information by rejecting any information that can identify the patient, either by the first method that requires the removal of specific identifiers of the patient or by the second statistical method where the patient verifies himself that enough identifiers are deleted. Nonetheless, an attacker can possibly get more external information assistance for de-identification in big data. As a result, de-identification is not sufficient for protecting big data privacy. It could be more feasible through developing efficient privacy-preserving algorithms to help mitigate the risk of re-identification. The concepts of k-anonymity [[46](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7" \l "ref-CR46" \o "Li N, et al. t-Closeness: privacy beyond k-anonymity and L-diversity. In: Data engineering (ICDE) IEEE 23rd international conference. 2007.),[47](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7" \l "ref-CR47" \o ),[48](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR48" \o "Samarati P. Protecting respondent’s privacy in microdata release. IEEE Trans Knowl Data Eng. 2001;13(6):1010–27.)], l-diversity [[47](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR47" \o ), [49](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR49" \o "Machanavajjhala A, Gehrke J, Kifer D, Venkitasubramaniam M. L-diversity: privacy beyond k-anonymity. In: Proc. 22nd international conference data engineering (ICDE). 2006. p. 24.), [50](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR50" \o "Samarati P, Sweeney L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical Report SRI-CSL-98-04, SRI Computer Science Laboratory. 1998.)] and t-closeness [[46](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR46" \o "Li N, et al. t-Closeness: privacy beyond k-anonymity and L-diversity. In: Data engineering (ICDE) IEEE 23rd international conference. 2007.), [50](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR50" \o "Samarati P, Sweeney L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical Report SRI-CSL-98-04, SRI Computer Science Laboratory. 1998.)] have been introduced to enhance this traditional technique.

k-anonymity In this technique, the higher the value of k, the lower will be the probability of re-identification. However, it may lead to distortions of data and hence greater information loss due to k-anonymization. Furthermore, excessive anonymization can make the disclosed data less useful to the recipients because some of the analysis becomes impossible or may produce biased and erroneous results. In k-anonymization, if the quasi-identifiers containing data are used to link with other publicly available data to identify individuals, then the sensitive attribute (like disease) as one of the identifier will be revealed. Table [3](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab3) is a non-anonymized database consisting of the patient records of some fictitious hospital in Casablanca.



There are six attributes along with five records in this data. There are two regular techniques for accomplishing k-anonymity for some value of k.

The first one is Suppression: in this method, an asterisk ‘\*’ could supplant certain values of the attributes. All or some of the values of a column may be replaced by ‘\*’. In the anonymized Table [4](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab4), replaced each of the values in the ‘Name’ attribute and all the values in the ‘Religion’ attribute by a ‘\*’.



The second method is Generalization: In this method, individual values of attributes are replaced with a broader category. For instance, The Birth field has been generalized to the year (e.g. the value ‘21/11/1972’ of the attribute ‘Birth’ may be supplanted by the year ‘1972’). The ZIP Code field has been also generalized to indicate the wider area (Casablanca).

Table [4](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab4) has 2-anonymity with respect to the attributes ‘Birth’, ‘Sex’ and ‘ZIP Code’ since for any blend of these attributes found in any row of the table there are always no less than two rows with those exact attributes. Each “quasi-identifier” tuple occurs in at least k records for a dataset with k-anonymity. k-anonymous data can still be helpless against attacks like unsorted matching attack, temporal attack, and complementary release attack [[50](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR50" \o "Samarati P, Sweeney L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical Report SRI-CSL-98-04, SRI Computer Science Laboratory. 1998.), [51](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR51" \o "Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness. 2002;10(5):557–70.)]. On the bright side, the complexity of rendering relations of private records k-anonymous, while minimizing the amount of information that is not released and simultaneously ensure the anonymity of individuals up to a group of size k, and withhold a minimum amount of information to achieve this privacy level and this optimization problem is NP-hard [[52](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR52" \o "Meyerson A, Williams R. On the complexity of optimal k-anonymity. In: Proc. of the ACM Symp. on principles of database systems. 2004.)].

Various measures have been proposed to quantify information loss caused by anonymization, but they do not reflect the actual usefulness of data [[53](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR53" \o "Iyenger V. Transforming data to satisfy privacy constraints. In: Proceedings of the ACM SIGKDD. 2002;279–88.), [54](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR54" \o "LeFevre K, Ramakrishnan R, DeWitt DJ. Mondrian multidimensional k-anonymity. In: Proceedings of the ICDE. 2006. p. 25.)]. Therefore, we move towards L-diversity strategy of data anonymization.

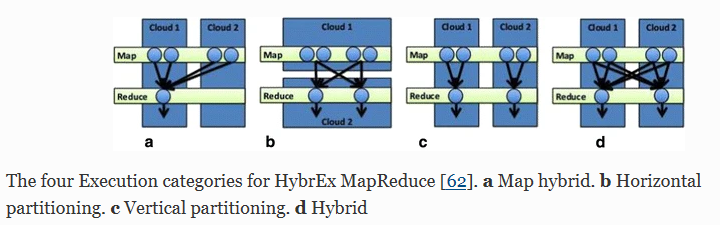
L-diversity It is a form of group based anonymization that is utilized to safeguard privacy in data sets by diminishing the granularity of data representation. This model (Distinct, Entropy, Recursive) [[46](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR46" \o "Li N, et al. t-Closeness: privacy beyond k-anonymity and L-diversity. In: Data engineering (ICDE) IEEE 23rd international conference. 2007.), [47](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR47" \o ), [51](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR51" \o "Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness. 2002;10(5):557–70.)] is an extension of the k-anonymity which utilizes methods including generalization and suppression to reduce the granularity of data representation in a way that any given record maps onto at least k different records in the data. The l-diversity model handles a few of the weaknesses in the k-anonymity model in which protected identities to the level of k-individuals is not equal to protecting the corresponding sensitive values that were generalized or suppressed. The problem with this method is that it depends upon the range of sensitive attribute. If want to make data L-diverse though sensitive attribute has not as much as different values, fictitious data to be inserted. This fictitious data will improve the security but may result in problems amid analysis. As a result, L-diversity method is also a subject to skewness and similarity attack [[51](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR51" \o "Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness. 2002;10(5):557–70.)] and thus can’t prevent attribute disclosure.

closeness Is a further improvement of l-diversity group based anonymization. The t-closeness model (equal/hierarchical distance) [[46](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR46" \o "Li N, et al. t-Closeness: privacy beyond k-anonymity and L-diversity. In: Data engineering (ICDE) IEEE 23rd international conference. 2007.), [50](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR50" \o "Samarati P, Sweeney L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical Report SRI-CSL-98-04, SRI Computer Science Laboratory. 1998.)] extends the l-diversity model by treating the values of an attribute distinctly, taking into account the distribution of data values for that attribute. The main advantage of this technique is that it intercepts attribute disclosure, and its problem is that as size and variety of data increase, the odds of re-identification increase too.

#### **B. HybrEx**

Hybrid execution model [[55](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR55" \o "Priyank J, Manasi G, Nilay K. Big data privacy: a technological perspective and review. J Big Data. 2016;3:25.)] is a model for confidentiality and privacy in cloud computing. It utilizes public clouds only for an organization’s non-sensitive data and computation classified as public, i.e., when the organization declares that there is no privacy and confidentiality risk in exporting the data and performing computation on it using public clouds, whereas for an organization’s sensitive, private data and computation, the model executes their private cloud. Moreover, when an application requires access to both the private and public data, the application itself also gets partitioned and runs in both the private and public clouds. It considers data sensitivity before a job’s execution and provides integration with safety.

The four categories in which HybrEx MapReduce enables new kinds of applications that utilize both public and private clouds are as shown in Fig. [2](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Fig2):



1. Map hybrid (1a) The map phase is executed in both the public and the private clouds while the reduce phase is executed in only one of the clouds.

2. Vertical partitioning (1b) Map and reduce tasks are executed in the public cloud using public data as the input, shuffle intermediate data amongst them, and store the result in the public cloud. The same work is done in the private cloud with private data. The jobs are processed in isolation.

3. Horizontal partitioning (1c) The map phase is executed only in public clouds, while the reduce phase is executed in a private cloud.

4. Hybrid (1d) The map phase and the reduce phase are executed on both public and private clouds. Data transmission among the clouds is also possible.

The problem with HybridEx is that it does not deal with the key that is generated at public and private clouds in the map phase and that it deals only with cloud as an adversary [[55](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR55" \o "Priyank J, Manasi G, Nilay K. Big data privacy: a technological perspective and review. J Big Data. 2016;3:25.)].

1. **Identity based anonymization**

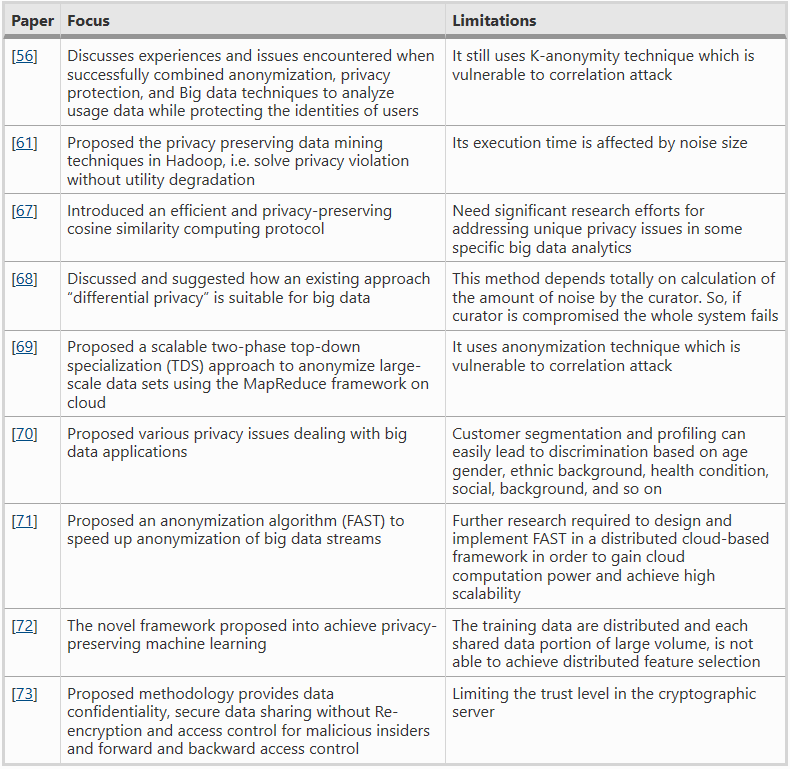
It is a type of information sanitization whose intent is privacy protection. It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous. The main difficulty with this technique involves combining anonymization, privacy protection, and big data techniques [[56](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR56" \o "Sedayao J, Bhardwaj R. Making big data, privacy, and anonymization work together in the enterprise: experiences and issues. In: Big data congress. 2014.)] to analyze usage data while protecting the identities.

Intel Human Factors Engineering team needed to protect Intel employees’ privacy using web page access logs and big data tools to enhance convenience of Intel’s heavily used internal web portal. They were required to remove personally identifying information (PII) from the portal’s usage log repository but in a way that did not influence the utilization of big data tools to do analysis or the ability to re-identify a log entry in order to investigate unusual behavior.

To meet the significant benefits of Cloud storage [[57](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR57" \o "Yong Yu, et al. Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Gen Comput Syst. 2016;62:85–91.)], Intel created an open architecture for anonymization [[56](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR56" \o "Sedayao J, Bhardwaj R. Making big data, privacy, and anonymization work together in the enterprise: experiences and issues. In: Big data congress. 2014.)] that allowed a variety of tools to be utilized for both de-identifying and re-identifying web log records. In the implementing architecture process, enterprise data has properties different from the standard examples in anonymization literature [[58](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR58" \o )]. Intel also found that in spite of masking obvious Personal Identification Information like usernames and IP addresses, the anonymized data was defenseless against correlation attacks. After exploring the tradeoffs of correcting these vulnerabilities, they found that User Agent information strongly correlates to individual users. This is a case study of anonymization implementation in an enterprise, describing requirements, implementation, and experiences encountered when utilizing anonymization to protect privacy in enterprise data analyzed using big data techniques. This investigation of the quality of anonymization used k-anonymity based metrics. Intel used Hadoop to analyze the anonymized data and acquire valuable results for the Human Factors analysts [[59](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR59" \o ), [60](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR60" \o )]. At the same time, it learned that anonymization needs to be more than simply masking or generalizing certain fields—anonymized datasets need to be carefully analyzed to determine whether they are vulnerable to attack.

### **Summary on recent approaches used in big data privacy**

In this paper, we have investigated the security and privacy challenges in big data, by discussing some existing approaches and techniques for achieving security and privacy in which healthcare organizations are likely to be highly beneficial. In this section, we focused on citing some approaches and techniques presented in different papers with emphasis on their focus and limitations (Table [5](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "Tab5)). Paper [[61](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR61" \o "Jung K, Park S, Park S. Hiding a needle in a haystack: privacy preserving Apriori algorithm in MapReduce framework PSBD’14, Shanghai. 2014. p. 11–7.)] for example, proposed privacy preserving data mining techniques in Hadoop. Paper [[67](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR67" \o "Lu R, Zhu H, Liu X, Liu JK, Shao J. Toward efficient and privacy-preserving computing in big data era. IEEE Netw. 2014;28:46–50.)] introduced also an efficient and privacy-preserving cosine similarity computing protocol and paper [[68](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR68" \o )] discussed how an existing approach “differential privacy” is suitable for big data. Moreover, paper [[69](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR69" \o "Zhang X, Yang T, Liu C, Chen J. A scalable two-phase top-down specialization approach for data anonymization using systems, in MapReduce on cloud. IEEE Trans Parallel Distrib. 2014;25(2):363–73.)] suggested a scalable approach to anonymize large-scale data sets. Paper [[70](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR70" \o "Mehmood A, Natgunanathan I, Xiang Y, Hua G, Guo S. Protection of big data privacy. In: IEEE translations and content mining are permitted for academic research. 2016.)] proposed various privacy issues dealing with big data applications, while paper [[71](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR71" \o "Mohammadian E, Noferesti M, Jalili R. FAST: fast anonymization of big data streams. In: ACM proceedings of the 2014 international conference on big data science and computing, article 1. 2014.)] proposed an anonymization algorithm to speed up anonymization of big data streams. In addition, paper [[72](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR72" \o "Xu K, Yue H, Guo Y, Fang Y. Privacy-preserving machine learning algorithms for big data systems. In: IEEE 35th international conference on distributed systems. 2015.)] suggested a novel framework to achieve privacy-preserving machine learning and paper [[73](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR73" \o "Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing. Inf Sci. 2014;258:371–86.)] proposed methodology provides data confidentiality and secure data sharing. All these techniques and approaches have shown some limitations.

****

These increased complexity and limits make the new models more difficult to interpret and their reliability less easy to assess, compared to previous models.

**Conclusion**

Whereas the potential opportunities offered for big data in the healthcare arena are unlimited (e.g. drive health research, knowledge discovery, clinical care, and personal health management), there are several obstacles that impede its true potential, including technical challenges, privacy and security issues and skilled talent. Big data security and privacy are considered huge obstacles for researchers in this field.

In this paper, we have briefly discussed some successful related work across the world. We have also presented privacy and security issues in each phase of big data lifecycle along with the advantages and flaws of existing technologies in the context of big healthcare data privacy and security.

We mainly reviewed the privacy preservation methods that have been used recently in healthcare and discussed how encryption and anonymization methods have been used for health care data protection as well as presented their limitations. Additionally, there are more various techniques include hiding a needle in a haystack [[61](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7?shared-article-renderer" \l "ref-CR61" \o "Jung K, Park S, Park S. Hiding a needle in a haystack: privacy preserving Apriori algorithm in MapReduce framework PSBD’14, Shanghai. 2014. p. 11–7.)], Attribute based encryption Access control, Homomorphic encryption, Storage path encryption and so on. However, the problem is always imposed.

In this context, as our future direction, perspectives consist in achieving effective solutions in privacy and security in the era of big healthcare data. As well, privacy methods need to be enhanced.

Also with the rapid development of IoT, the greater the quantity, the lower the quality. Consequently, quality of data should not be affected more by privacy preserving algorithms to get the appropriate result by researchers. And to go further, we will try to solve the problem of reconciling security and privacy models by simulating diverse approaches to ultimately support decision making and planning strategies.

References

1.Burghard C. Big data and analytics key to accountable care success. Framingham: IDC Health Insights; 2012.

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Big data and analytics key to accountable care success&publication_year=2012&author=Burghard,C)

2.Fernandes L, O’Connor M, Weaver V. Big data, bigger outcomes. J AHIMA. 2012;83:38–42.

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Big data, bigger outcomes&journal=J AHIMA.&volume=83&pages=38-42&publication_year=2012&author=Fernandes,L&author=O%E2%80%99Connor,M&author=Weaver,V)

3.David Houlding, MSc, CISSP. Health Information at Risk: Successful Strategies for Healthcare Security and Privacy. Healthcare IT Program Of ce Intel Corporation, white paper. 2011.

4.South Tyneside NHS Foundation Trust. Harnessing analytics for strategic planning, operational decision making and end-to-end improvements in patient care. IBM Smarter Planet brief. 2013.

5.UNC Health Care relies on analytics to better manage medical data and improve patient care. IBM Press release. 2013.

6.Indiana Health Information Exchange. <http://www.ihie.org/>. Accessed 24 Mar 2016.

7.Transforming healthcare through big data, strategies for leveraging big data in the healthcare industry. Institute for Health. 2013.

8.Artemis. <http://hir.uoit.ca/cms/?q=node/24>. Accessed 21 May 2016.

9.Groves P, Kayyali B, Knott D, Kuiken SV. The big data revolution in healthcare, accelerating value and innovation. 2013.

10.WHO. Mobile phones help people with diabetes to manage fasting and feasting during Ramadan. Features. 2014.

11.Sophia Genetics. «Product & Technology Overview» 2014.

12.

Sophia Genetics. <http://www.sophiagenetics.com/news/media-mix/details/news/african-hospitals-adopt-sophia-artificial-intelligence-to-trigger-continent-wide-healthcare-leapfrogging-movement.html>. Accessed 24 Mar 2017.

13.CynergisTek, Redspin. «BREACH REPORT 2016: Protected Health Information (PHI)» 2017.

14.Podesta J, et al. Big data: seizing opportunities, preserving values. Executive Office of the President. 2014;1:2013.

15.House W. Big data and privacy: a technological perspective. Washington: Executive Office of the President, President’s Council of Advisors on Science and Technology; 2014.

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Big data and privacy: a technological perspective&publication_year=2014&author=House,W)

16.House W. FACT SHEET: big data and privacy working group review. 2014.

17.OECD. Data-driven healthcare innovation, management and policy, DELSA/HEA(2013)13. Paris: OECD; 2013.

18.Kim S-H, Kim N-U, Chung T-M. Attribute relationship evaluation methodology for big data security. In: 2013 international conference on IT convergence and security (ICITCS), IEEE. p. 1–4. <https://xs.scihub.ltd/https://doi.org/10.1109/icitcs.2013.6717808>.

19.“Data-driven healthcare organizations use big data analytics for big gains” IBM white paper February. 2013.

20.Yazan A, Yong W, Raj Kumar N. Big data life cycle: threats and security model. In: 21st Americas conference on information systems. 2015.

21.Xu L, Jiang C, Wang J, Yuan J, Ren Y. Information security in big data: privacy and data mining. J Rapid Open Access Publ. 2014;2:1149–76. <https://xs.scihub.ltd/https://doi.org/10.1109/ACCESS.2014.2362522>.

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Information security in big data: privacy and data mining&journal=J Rapid Open Access Publ&doi=10.1109/ACCESS.2014.2362522&volume=2&pages=1149-1176&publication_year=2014&author=Xu,L&author=Jiang,C&author=Wang,J&author=Yuan,J&author=Ren,Y)

22.General Dynamics Health Solutions white paper UK. “Securing Big Health Data”©2015. <http://gdhealth.com/globalassets/health-solutions/documents/brochures/securing-big-health-data_-white-paper_UK.pdf>.

23.Zhang R, Liu L. Security models and requirements for healthcare application clouds. In: IEEE 3rd international conference on cloud computing. 2010.

24.Shafer J, Rixner S, Cox AL. The hadoop distributed filesystem: balancing portability and performance. In: Proceedings of 2010 IEEE international symposium on performance analysis of systems & software (ISPASS), March 2010, White Plain, NY. p. 122–33.

25.Yang C, Lin W, Liu M. A novel triple encryption scheme for hadoop-based cloud data security. In: Emerging intelligent data and web technologies (EIDWT), 2013 fourth international conference on. 2013. p. 437–42.

26.Federal Information Processing Standards Publication 197. Specification for the advanced encryption standards (AES). 2001.

27.Somu N, Gangaa A, Sriram VS. Authentication service in hadoop using one time pad. Indian J Sci Technol. 2014;7:56–62.

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Authentication service in hadoop using one time pad&journal=Indian J Sci Technol&volume=7&pages=56-62&publication_year=2014&author=Somu,N&author=Gangaa,A&author=Sriram,VS)

28.Fluhrer S, Mantin I, Shamir A. Weakness in the key scheduling algorithm of RC4. In: 8th annual international workshop on selected areas in cryptography, London: Springer-Verlag. 2001.

29.Sweeney L. Achieving k-anonymity privacy protection using generalization and suppression. Int J Uncertain Fuzziness Knowl Based Syst. 2002;10:571–88.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=1948200)

[Article](https://xs.scihub.ltd/https://doi.org/10.1142/S021848850200165X)

[MATH](http://www.emis.de/MATH-item?1084.68537)

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Achieving k-anonymity privacy protection using generalization and suppression&journal=Int J Uncertain Fuzziness Knowl Based Syst.&volume=10&pages=571-588&publication_year=2002&author=Sweeney,L)

30.Samrati P. Protecting respondents identities in microdata release. IEEE Trans Knowl Data Eng. 2001;13:1010–27.

[Article](https://xs.scihub.ltd/https://doi.org/10.1109/69.971193)

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Protecting respondents identities in microdata release&journal=IEEE Trans Knowl Data Eng&volume=13&pages=1010-1027&publication_year=2001&author=Samrati,P)

31.Truta TM, Vinay B. Privacy protection: p-sensitive k-anonymity property. In: Proceedings of 22nd international conference on data engineering workshops. 2006. p. 94.

32.Spruill N. The confidentiality and analytic usefulness of masked business microdata. In: Proceedings on survey research methods. 1983. p. 602–607.

33.Chawala S, Dwork C, Sheny FM, Smith A, Wee H. Towards privacy in public databases. In: Proceedings on second theory of cryptography conference. 2005.

34.Science Applications International Corporation (SAIC). Role-based access control (RBAC) Role Engineering Process Version 3.0. 2004.

35.Mohan A, Blough DM. An attribute-based authorization policy framework with dynamic conflict resolution. In: Proceedings of the 9th symposium on identity and trust on the internet. 2010.

36.Hagner M. Security infrastructure and national patent summary. In: Tromso telemedicine and eHealth conference. 2007.

37.Zhou H, Wen Q. Data security accessing for HDFS based on attribute-group in cloud computing. In: International conference on logistics engineering, management and computer science (LEMCS 2014). 2014.

38.Linden H, Kalra D, Hasman A, Talmon J. Inter-organization future proof HER systems—a review of the security and privacy related issues. Int J Med Inform. 2009;78:141–60.

[Article](https://xs.scihub.ltd/https://doi.org/10.1016/j.ijmedinf.2008.06.013)

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Inter-organization future proof HER systems%E2%80%94a review of the security and privacy related issues&journal=Int J Med Inform&volume=78&pages=141-160&publication_year=2009&author=Linden,H&author=Kalra,D&author=Hasman,A&author=Talmon,J)

39.Marchal S, Xiuyan J, State R, Engel T. “A big data architecture for large scale security monitoring”, Big Data (BigData Congress), Anchorage, AK. 2014. p. 56–63.

40.Duygu ST, Ramazan T, Seref S. A survey on security and privacy issues in big data. In: The 10th international conference for internet technology and secured transactions (ICITST-2015).

41.Liu L, Lin J. Some special issues of network security monitoring on big data environments. Dependable, Autonomic and Secure Computing (DASC), Chengdu. 2013. p. 10–5.

42.Hill K. How target figured out a teen girl was pregnant before her father did. Forbes, Inc. 2012.

43.Big Data security and privacy issues in healthcare—Harsh KupwadePatil, Ravi Seshadri. 2014.

44.Sectorial healthcare strategy 2012–2016-Moroccan healthcare ministry.

45.Patil P, Raul R, Shroff R, Maurya M. Big data in healthcare. 2014.

46.Li N, et al. t-Closeness: privacy beyond k-anonymity and L-diversity. In: Data engineering (ICDE) IEEE 23rd international conference. 2007.

47.Ton A, Saravanan M. Ericsson research. .<http://www.ericsson.com/research-blog/data-knowledge/big-data-privacy-preservation/2015>.

48.Samarati P. Protecting respondent’s privacy in microdata release. IEEE Trans Knowl Data Eng. 2001;13(6):1010–27.

[Article](https://xs.scihub.ltd/https://doi.org/10.1109/69.971193)

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Protecting respondent%E2%80%99s privacy in microdata release&journal=IEEE Trans Knowl Data Eng&volume=13&issue=6&pages=1010-1027&publication_year=2001&author=Samarati,P)

49.Machanavajjhala A, Gehrke J, Kifer D, Venkitasubramaniam M. L-diversity: privacy beyond k-anonymity. In: Proc. 22nd international conference data engineering (ICDE). 2006. p. 24.

50.Samarati P, Sweeney L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical Report SRI-CSL-98-04, SRI Computer Science Laboratory. 1998.

51.Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness. 2002;10(5):557–70.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=1948199)

[Article](https://xs.scihub.ltd/https://doi.org/10.1142/S0218488502001648)

[MATH](http://www.emis.de/MATH-item?1085.68589)

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=K-anonymity: a model for protecting privacy&journal=Int J Uncertain Fuzziness&volume=10&issue=5&pages=557-570&publication_year=2002&author=Sweeney,L)

52.Meyerson A, Williams R. On the complexity of optimal k-anonymity. In: Proc. of the ACM Symp. on principles of database systems. 2004.

53.Iyenger V. Transforming data to satisfy privacy constraints. In: Proceedings of the ACM SIGKDD. 2002;279–88.

54.LeFevre K, Ramakrishnan R, DeWitt DJ. Mondrian multidimensional k-anonymity. In: Proceedings of the ICDE. 2006. p. 25.

55.Priyank J, Manasi G, Nilay K. Big data privacy: a technological perspective and review. J Big Data. 2016;3:25.

[Article](https://xs.scihub.ltd/https://doi.org/10.1186/s40537-016-0059-y)

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Big data privacy: a technological perspective and review&journal=J Big Data.&volume=3&publication_year=2016&author=Priyank,J&author=Manasi,G&author=Nilay,K)

56.Sedayao J, Bhardwaj R. Making big data, privacy, and anonymization work together in the enterprise: experiences and issues. In: Big data congress. 2014.

57.Yong Yu, et al. Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Gen Comput Syst. 2016;62:85–91.

[Article](https://xs.scihub.ltd/https://doi.org/10.1016/j.future.2016.02.003)

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Cloud data integrity checking with an identity-based auditing mechanism from RSA&journal=Future Gen Comput Syst.&volume=62&pages=85-91&publication_year=2016&author=Yong,Yu)

58.Oracle big data for the enterprise. 2012. <http://www.oracle.com/ca-en/technoloqies/biq-doto>.

59.Hadoop Tutorials. 2012. <https://developer.yahoo.com/hadoop/tutorial>.

60.Fair scheduler guide. 2013. <http://hadoop.apache.org/docs/r0.20.2/fair_scheduler.html>.

61.Jung K, Park S, Park S. Hiding a needle in a haystack: privacy preserving Apriori algorithm in MapReduce framework PSBD’14, Shanghai. 2014. p. 11–7.

62.Ko SY, Jeon K, Morales R. The HybrEx model for confidentiality and privacy in cloud computing. In: 3rd USENIX workshop on hot topics in cloud computing, HotCloud’11, Portland. 2011.

63.Data Protection Laws of the World. 2017 DLA Piper. <http://www.dlapiperdataprotection.com>.

64.Privacy and Big Data—Terence Craig & Mary E. Ludloff.

65.Challenges of privacy protection in big data analytics—Meiko Jensen-2013 IEEE international congress on big data. 2013.

66.Data protection overview (Morocco)—Florence Chafiol-Chaumont and Anne-Laure Falkman. 2013.

67.Lu R, Zhu H, Liu X, Liu JK, Shao J. Toward efficient and privacy-preserving computing in big data era. IEEE Netw. 2014;28:46–50.

[Article](https://xs.scihub.ltd/https://doi.org/10.1109/MNET.2014.6863131)

[Google Scholar](http://f.glgoo.top/scholar_lookup?&title=Toward efficient and privacy-preserving computing in big data era&journal=IEEE Netw.&volume=28&pages=46-50&publication_year=2014&author=Lu,R&author=Zhu,H&author=Liu,X&author=Liu,JK&author=Shao,J)

68.Microsoft differential privacy for everyone. 2015. [http://download.microsoft.com/…/Differential\_Privacy\_for\_Everyone.pdf](http://download.microsoft.com/%e2%80%a6/Differential_Privacy_for_Everyone.pdf).

69.Zhang X, Yang T, Liu C, Chen J. A scalable two-phase top-down specialization approach for data anonymization using systems, in MapReduce on cloud. IEEE Trans Parallel Distrib. 2014;25(2):363–73.

70.Mehmood A, Natgunanathan I, Xiang Y, Hua G, Guo S. Protection of big data privacy. In: IEEE translations and content mining are permitted for academic research. 2016.

71.Mohammadian E, Noferesti M, Jalili R. FAST: fast anonymization of big data streams. In: ACM proceedings of the 2014 international conference on big data science and computing, article 1. 2014.

72.Xu K, Yue H, Guo Y, Fang Y. Privacy-preserving machine learning algorithms for big data systems. In: IEEE 35th international conference on distributed systems. 2015.

73.Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing. Inf Sci. 2014;258:371–8

**译文：**

**21世纪计算机：当前安全和隐私挑战**

[互联网服务与应用杂志](https://jisajournal.springeropen.com/) 9，文章编号：24（2018）

**摘要**

自从马克·威瑟在21世纪的电脑上发表他有影响力的作品以来，几十年过去了。多年来，该文件中提出的一些UbiComp功能已逐渐被技术市场上的行业参与者所采用。虽然这种技术演变给我们的社会带来了许多好处，但它也带来了无数我们尚未超越的挑战。在本文中，我们将讨论来自影响 UbiComp 革命最多的领域的主要挑战：

1. 软件保护：弱类型语言、多语种软件和联网嵌入式系统。

2. 长期安全：密码分析和量子攻击的最新进展。

3. 加密工程：轻量级密码系统及其安全实现。

4. 恢复能力：与服务可用性和弹性的至高无上作用有关的问题。

5. 隐私含义：敏感性数据识别和监管。

6. 法证：来自数字和物理世界协同作用的可信证据。

我们指明了解决这些问题的方向，并声称如果我们把这一切正确对待，我们将把UbiComp的科幻小说变成科学事实。

**介绍**

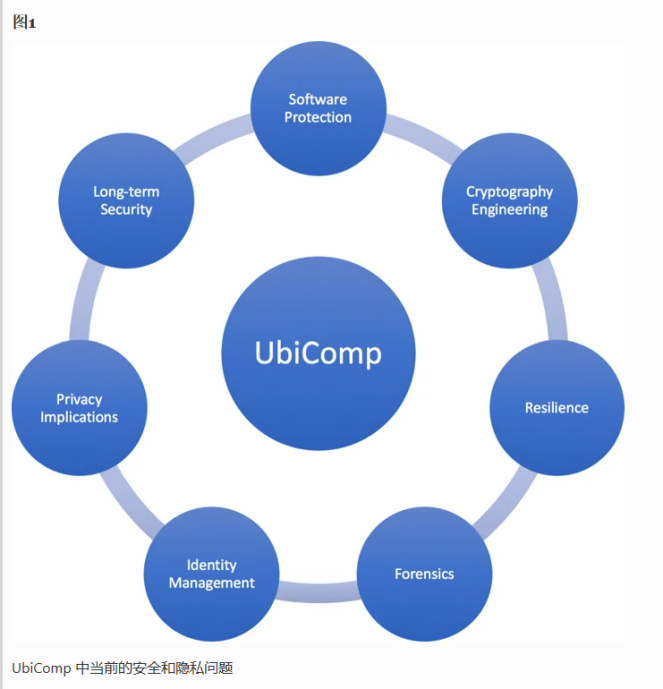
1991年，马克·威瑟描述了*21世纪计算机*的愿景[[1]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR1" \o "Weiser M. The computer for the 21st century. Sci Am. 1991; 265(3):94–104.)Weiser在他的预言论文中认为，影响最深远的技术是那些让自己消失、消失在稀薄空气中的技术。根据Weiser的说法，这种遗忘是一种人类现象，而不是技术现象："每当人们学到足够好的东西时，他们就不再意识到这一点，"他声称。此事件称为"隐性维度"或"编译"，例如，当司机对路标做出反应时，无意识地处理字母S-T-O-P[1]。

然而，四分之一个世纪后，威瑟的梦想远未实现。多年来，他关于普及和无处不在的计算（UbiComp）[[2](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR2" \o "Weiser M. Some computer science issues in ubiquitous computing. Commun ACM. 1993; 36(7):75–84.)， [3](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR3" \o "Lyytinen K, Yoo Y. Ubiquitous computing. Commun ACM. 2002; 45(12):63–96.)]的许多概念已经具体化到今天我们称之为无线传感器网络[[4](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR4" \o "Estrin D, Govindan R, Heidemann JS, Kumar S. Next century challenges: Scalable coordination in sensor networks. In: MobiCom’99. New York: ACM: 1999. p. 263–70.)，[5](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR5" \o "Pottie GJ, Kaiser WJ. Wireless integrated network sensors. Commun ACM. 2000; 43(5):51–8.)]，物联网[[6，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR6" \o "Ashton K. That ’Internet of Things’ Thing. RFiD J. 2009; 22:97–114.)[7](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR7" \o "Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput Netw. 2010; 54(15):2787–805.)]，可穿戴设备[[8，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR8" \o "Mann S. Wearable computing: A first step toward personal imaging. Computer. 1997; 30(2):25–32.)[9]](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR9" \o "Martin T, Healey J. 2006’s wearable computing advances and fashions. IEEE Pervasive Comput. 2007; 6(1):14–6.)和网络物理系统[[10，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR10" \o "Lee EA. Cyber-physical systems-are computing foundations adequate. In: NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, volume 2. Citeseer: 2006.)[11](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR11" \o "Rajkumar RR, Lee I, Sha L, Stankovic J. Cyber-physical systems: the next computing revolution. In: 47th Design Automation Conference. ACM: 2010.)]。这些系统的应用范围从交通事故和CO2 排放监测到自动驾驶汽车和病人家庭护理。然而，除了它们的所有好处外，这些系统本身的出现也带来了一些缺点。而且，除非我们适当地解决这些问题，否则威瑟预言的连续性将岌岌可危。

UbiComp带来了新的缺点，因为与传统计算相比，它呈现出完全不同的前景 [[12](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR12" \o "Abowd GD, Mynatt ED. Charting past, present, and future research in ubiquitous computing. ACM Trans Comput Human Interact (TOCHI). 2000; 7(1):29–58.)] 。例如，UbiComp 中的计算机系统具有传感器、CPU 和执行器。相应地，这意味着他们可以听到（或窥探）用户，处理她/他的数据（并可能找出一些关于她/他的秘密），并回应她/他的行为（或者，最终，通过揭示一些秘密暴露他/他）。这些功能反过来又为不适合 UbiComp 环境的传统计算机提出建议，并带来了新的挑战。

在上述方案中，一些最关键的挑战在于安全和隐私领域[[13](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR13" \o "Stajano F. Security for ubiquitous computing.Hoboken: Wiley; 2002.)]。这是因为市场和用户往往追求一个功能齐全的系统，而牺牲了适当的操作和保护;相反，随着计算元素渗透到我们的日常生活中，对更强大的安全方案的需求比以往任何时候都要大。值得注意的是，迫切需要一个安全机制，能够涵盖UbiComp的所有方面和表现，跨越时间和空间，以无缝和有效的方式。

在本文中，我们将在UbiComp（图[1）](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig1)的背景下讨论当代的安全和隐私问题。我们研究多个尚未解决的问题，并指出有希望的方法解决他们的解决方案。更确切地说，我们调查以下挑战及其后果。

图一

1. 第[2](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec2)节中的软件保护：我们研究了资源受限设备采用弱类型语言的影响，并讨论了减轻这种影响的机制。我们介绍验证多语言软件（即基于多种编程语言的软件）的技术，并重新审视分析网络嵌入式系统的有前途的方法。

2. 第[3](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec6)节中的长期安全性：我们研究当今广泛使用的加密系统（例如，基于 RSA 和 ECC）的安全性，提出一些最新的威胁（例如，密码分析和量子攻击的进步），并探索新的方向和挑战，以保证 UbiComp 环境中的长期安全性。

3. 第[4](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec10)节：我们重新强调了加密在保护计算机中的重要作用，讨论了轻量级加密系统的现状及其安全实现，并强调了密钥管理协议中的挑战。

4. 第[5](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec14)节中的弹性：我们强调与服务可用性相关的问题，并强调了在 UbiComp 环境中弹性的重要性。

5. 第6节中的隐私影响：我们解释了为什么安全是必要的，但不足以确保隐私，讨论重要的隐私相关问题（例如，敏感性数据识别和监管），并讨论一些交易工具来解决这些问题（例如，基于同构加密的隐私保护协议）。

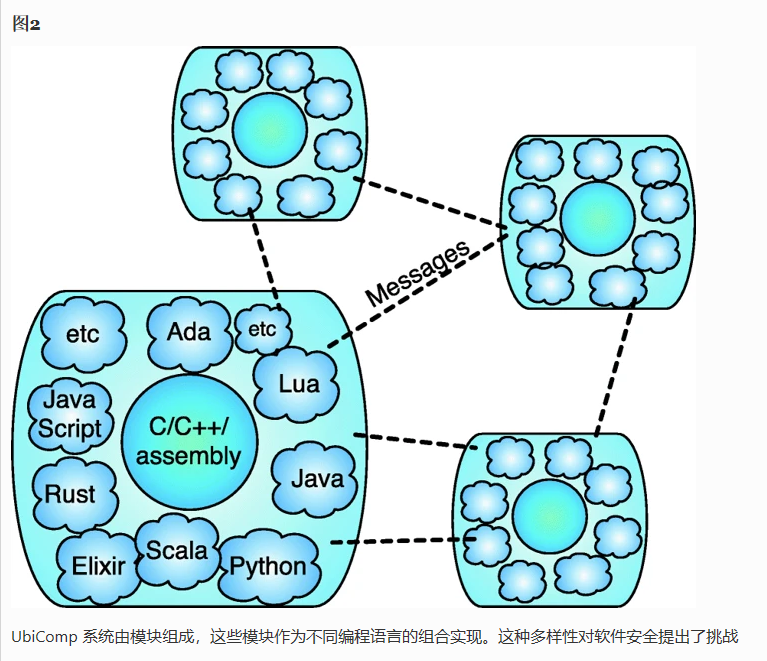
6. 第7节中的取证，我们介绍了协同使用物理和数字证据以促进网络系统可信操作的好处。

我们相信，只有正确应对这些挑战，我们才能将UbiComp的科幻小说转化为科学事实。

特别是，我们选择解决上述领域，因为它们代表了有前途的研究方向，例如涵盖 UbiComp 安全和隐私的不同方面。

**软件保护**

现代 UbiComp 系统很少从头开始构建。不同组织开发的组件，具有不同的编程模型和工具，并在不同的假设下集成，以提供复杂的功能。在本节中，我们将分析从这样一个世界中出现的软件生态系统。图[2](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig2)提供了此生态系统的高级表示形式。在本部分的其余部分中，我们将特别关注此环境的三个方面，这些方面对开发人员构成安全挑战：C 和 C++ 的安全缺陷，C 和 C++ 是网络物理实现中的主要编程语言;这些语言与其他编程语言之间的交互，以及这些交互对 UbiComp 应用程序的分布式性质的影响。我们首先深入探讨 C 和 C++ 的特点。

**类型安全**

UbiComp 系统中使用的大量软件用 C 或 C# 中实现。鉴于这两种编程语言具有无与伦比的效率，这一事实是自然的。但是，如果C和C++一方面产生高效的可执行文件，另一方面，它们的弱类型系统导致大量软件漏洞。在编程语言的argot中，我们说类型系统在不支持两个关键属性时是弱的：*进度*和*保*留[[14]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR14" \o "Pierce BC. Types and programming languages, 1st edition. Cambridge: The MIT Press; 2002.)这些属性的正式定义对于后面的讨论来说并不重要。只要知道，由于键入弱，C 或 C# 都不能确保有界内存访问。因此，用这些语言编写的程序可以访问无效的内存位置。为了说明这种可能性带来的危险，只需知道超出边界的访问是缓冲区溢出漏洞利用背后的原则就足够了。

软件安全社区一直在开发不同的技术来处理 C/C++/组装软件的内在漏洞。此类技术可以是完全静态的、完全动态的或两种方法的混合。静态保护机制在编译器级别实现;动态机制在运行时级别实现。在本部分的其余部分中，我们将列出每个类别中最知名的元素。

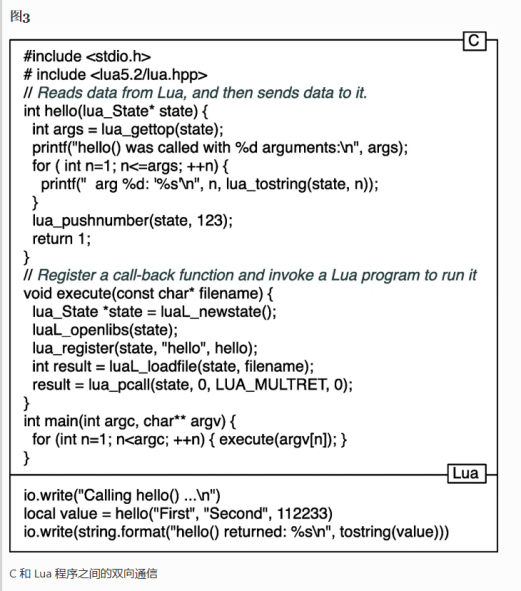
静态分析提供程序行为的保守估计，而无需执行此类程序。例如，这种广泛的技术系列包括抽象解释[[15](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR15" \o "Cousot P, Cousot R. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: POPL. New York: ACM: 1977. p. 238–52.)]、模型检查[[16](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR16" \o "McMillan KL. Symbolic model checking. Norwell: Kluwer Academic Publishers; 1993.)] 和引导性证明[[17](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR17" \o "Leroy X. Formal verification of a realistic compiler. Commun ACM. 2009; 52(7):107–15.)] 。静态分析的主要优点是运行时开销低，并且其健全性：推断的属性保证始终为 true。但是，静态分析也有缺点。特别是，大多数有趣的程序属性位于不可决定的土地 [[18](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR18" \o "Rice HG. Classes of recursively enumerable sets and their decision problems. Trans Amer Math Soc. 1953; 74(1):358–66.)] 。此外，许多正式属性的验证，即使是一个可计算的问题，也会产生令人望而却步的计算成本[[19](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR19" \o "Wilson RP, Lam MS. Efficient context-sensitive pointer analysis for c programs. In: PLDI. New York: ACM: 1995. p. 1–12.)] 。

动态分析有多种类型：测试（KLEE [[20](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR20" \o "Cadar C, Dunbar D, Engler D. KLEE: Unassisted and automatic generation of high-coverage tests for complex systems programs. In: OSDI. Berkeley: USENIX: 2008. p. 209–24.)]）、分析（Aprof [[21](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR21" \o "Coppa E, Demetrescu C, Finocchi I. Input-sensitive profiling. In: PLDI. New York: ACM: 2012. p. 89–98.)], Gprof [[22](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR22" \o "Graham SL, Kessler PB, McKusick MK. gprof: a call graph execution profiler (with retrospective). In: Best of PLDI. New York: ACM: 1982. p. 49–57.)]）、符号执行（DART [[23](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR23" \o "Godefroid P, Klarlund N, Sen K. Dart: directed automated random testing. In: PLDI. New York: ACM: 2005. p. 213–23.)]）、仿真（Valgrind [[24](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR24" \o "Nethercote N, Seward J. Valgrind: a framework for heavyweight dynamic binary instrumentation. In: PLDI. New York: ACM: 2007. p. 89–100.)]）和二进制检测（Pin [[25](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR25" \o "Luk C-K, Cohn R, Muth R, Patil H, Klauser A, Lowney G, Wallace S, Reddi VJ, Hazelwood K. Pin: Building customized program analysis tools with dynamic instrumentation. In: PLDI. New York: ACM: 2005. p. 190–200.)]）。动态分析的优点和局限性与静态技术中的优点和局限性完全相反。动态分析通常不会引发误报：错误通过示例描述，通常会导致一致的复制 [[26](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR26" \o "Rimsa AA, D’Amorim M, Pereira FMQ. Tainted flow analysis on e-SSA-form programs. In: CC. Berlin: Springer: 2011. p. 124–43.)] 。但是，它们不需要始终在软件中查找安全漏洞。此外，动态分析上方的粗糙度仍然使其无法将其应用于生产软件。

作为一个中间点，几个研究小组提出了将静态分析与动态分析相结合的方法，产生了不同类型的混合方法来保护低级代码。当单独使用 [[28](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR28" \o "Russo A, Sabelfeld A. Dynamic vs. static flow-sensitive security analysis. In: CSF. Washington: IEEE: 2010. p. 186–99.)] 时，这种组合可能会产生比静态或动态方法所能获得的安全保证更强大的保证。然而，负面的结果仍然存在：如果攻击者可以控制程序，通常他或她可以绕过最先进的混合保护机制，如控制流完整性 [[29](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR29" \o "Carlini N, Barresi A, Payer M, Wagner D, Gross TR. Control-flow bending: On the effectiveness of control-flow integrity. In: SEC. Berkeley: USENIX: 2015. p. 161–76.)] 。这一事实最终是UbiComp系统实施中通常看到的语言采用的弱类型系统的结果。因此，设计和部署能够保护此类编程语言的技术，而不损害其效率，使之不再足以用于 UbiComp 开发，仍然是一个悬而未决的问题。

在引导形式方法在编程语言的设计与实现中发挥较大作用的困难中，在这个领域已经取得了很大的成就。这一说法的证明是，今天研究人员能够确保整个操作系统内核的安全，如Gerwin等人[[30]](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR30" \o "Klein G, Elphinstone K, Heiser G, Andronick J, Cock D, Derrin P, Elkaduwe D, Engelhardt K, Kolanski R, Norrish M, Sewell T, Tuch H, Winwood S. sel4: Formal verification of an os kernel. In: SOSP. New York: ACM: 2009. p. 207–20.)所证明的，并确保编译器满足他们处理的语言的语义[[31]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR31" \o "Jourdan J-H, Laporte V, Blazy S, Leroy X, Pichardie D. A formally-verified c static analyzer. In: POPL. New York: ACM: 2015. p. 247–59.)不过，我们有理由认为，某些安全措施可能以性能为代价，因此，我们预期，未来数年，研究界的大部分努力，将致力使正式方法不仅更强大、更具表现力，而且更有效率，可在实践中使用。

**Polyglot编程**

Polyglot 编程是编写涉及两种或两种以上编程语言的源代码的艺术和学科。它在网络物理系统的实现中很常见。例如，巴西数字电视协议Ginga主要在Lua和C [[32](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR32" \o "Soares LFG, Rodrigues RF, Moreno MF. Ginga-NCL: the declarative environment of the brazilian digital tv system. J Braz Comp Soc. 2007; 12(4):1–10.)] 中实施。图[3](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig3)显示了 C 和 Lua 程序之间的通信示例。编程语言之间的其他交互示例包括 C 和 Python 之间的绑定 [[33](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR33" \o "Maas AJ, Nazaré H, Liblit B. Array length inference for c library bindings. In: ASE. New York: ACM: 2016. p. 461–71.)]、C 和 Elixir[[34](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR34" \o "Fedrecheski G, Costa LCP, Zuffo MK. ISCE. Washington: IEEE: 2016.)]和 Java 本机接口 [[35](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR35" \o "Rellermeyer JS, Duller M, Gilmer K, Maragkos D, Papageorgiou D, Alonso G. The software fabric for the internet of things. In: IOT. Berlin, Heidelberg: Springer-Verlag: 2008. p. 87–104.)]。多聚体编程使系统保护复杂化。由于缺乏多语言工具以及 C/C++ 和其他语言之间未检查的内存绑定，因此会出现困难。

多语种软件验证的一个障碍是缺乏在统一框架下分析用不同编程语言编写的源代码的工具。回到图[3，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig3)我们有一个由两个程序组成的系统，用不同的编程语言编写。任何分析整个系统的工具都必须能够分析这两个不同的语法并推断它们之间的连接点。为此已经开展了工作，但解决办法仍然非常初步。例如，Maas 等人 [[33](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR33" \o "Maas AJ, Nazaré H, Liblit B. Array length inference for c library bindings. In: ASE. New York: ACM: 2016. p. 461–71.)] 已经实现了自动方法来检查 Python 程序是否正确读取 C 数组。作为另一个例子，Furr 和 Foster [[36](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR36" \o "Furr M, Foster JS. Checking type safety of foreign function calls. ACM Trans Program Lang Syst. 2008; 30(4):18:1–18:63.)] 描述了确保 OCaml 到 C 和 Java 到 C 绑定的类型安全性的技术。

分析多语种系统的一个有希望的方向是基于部分可用的源代码编译的想法。此壮举包括重建缺失的语法和缺少的声明，以生成可以由典型工具分析的原始程序的最小版本。通过分析部分可用的代码，可以单独测试多语种程序的各个部分，从而产生整个系统的内聚视图。该技术已被证明可以生成可分析的Java源代码[[37]，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR37" \o "Dagenais B, Hendren L. OOPSLA. New York: ACM: 2008. p. 313–28.)可编译的C码[[38]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR38" \o "Melo LTC, Ribeiro RG, de Araújo MR, Pereira FMQ. Inference of static semantics for incomplete c programs. Proc ACM Program Lang. 2017; 2(POPL):29:1–29:28.)请注意，这种类型的重建并不限于高级编程语言。这一事实的见证是微观执行的概念，由帕特里斯·戈德夫罗伊德[[39]](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR39" \o "Godefroid P. Micro execution. In: ICSE. New York: ACM: 2014. p. 539–49.)介绍。Godefroid 的工具允许测试 x86 二进制文件，即使缺少对象文件也是如此。然而，尽管有这些发展，重建仍然局限于程序的静态语义。行为综合是计算机科学中蓬勃发展的学科[[40](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR40" \o "Manna Z, Waldinger RJ. Toward automatic program synthesis. Commun ACM. 1971; 14(3):151–65.)]，但仍远远没有实现多语种系统的认证。

**分布式编程**

无处不在的计算系统往往被分布式。甚至很难想象在这个世界上不与其他程序交互的应用程序的任何用途。众所周知，分布式编程为恶意用户打开了几扇门。因此，为了使网络物理技术更安全，安全工具必须了解此类系统的分布式性质。然而，这一要求面前面临两个主要挑战：难以构建分布式应用程序的整体视图，以及缺乏与通过网络通信的进程之间交换的消息绑定的语义信息。

准确地说，分布式系统的分析需要考虑构成该系统的几个程序部分之间的交互作用[41]。发现这种交互是很困难的，即使我们将自己限制在用单一编程语言编写的代码中。困难源于缺乏与发送和接收消息的操作相关联的语义信息。换句话说，这些操作被定义为库的一部分，而不是编程语言本身的一部分。尽管如此，有几种技术可以推断不同源代码片段之间的通信通道。例如，我们有Greg Bronevetsky[42]和Teixeira等人的算法[43]，它构建了程序控制流图（CFG）的分布式视图。经典的静态分析不需要对这个分布式CFG做进一步的修改。然而，分布式CFG仍然是程序行为的保守近似。因此，它强迫已经不精确的静态分析来处理在程序执行期间可能永远不存在的通信通道。基于actor的库的日益普及，比如Elixir[34]和Scala[44]等语言中的库，可能会缓解信道推断问题。在actor模型中，通道在组成分布式系统的不同处理元素之间交换的消息是显式的。然而，这种模式能否被物联网社区广泛采用，仍然是一个有待观察的事实。

在程序中执行自动分析的工具依赖于静态信息来产生更精确的结果。从这个意义上说，类型是理解软件的核心。例如，在Java和其他面向对象语言中，对象的类型决定了信息如何沿着程序代码流动。然而，尽管如此重要，在绝大多数分布式系统中交换的消息都不是类型化的。原因是这样的事实，至少在C、C++和汇编软件中，这些消息是字节数组。有两个主要的努力来缓解这个问题：将消息作为一级值添加到编程语言中，以及在缺乏这种特性的语言中实现能够处理指针算法的分析点。关于第一席，一些编程语言，如Scala、Erlang和IrxIR，将消息作为基本构造，为开发者提供了非常有表现力的方式来实现参与者模型（45）——分布式编程的核心基础。尽管围绕actor模型构建编程抽象并不是一个新的想法[45]，但它们的流行似乎是2000年代的一个现象，因为抽象的表达能力越来越强[46]，实现的效率越来越高[47]。在第二个方面，研究人员已经设计出分析方法来推断弱类型编程语言中数组的内容和大小。更重要的是，近年来出现了一系列新的算法来分析C/C++风格指针算法[50—53]。高级编程语言的广泛采用以及分析低级语言的新工具的构建是令人兴奋的。这一趋势似乎表明，编程语言界每次都更加关注实现更安全的分布式软件的任务。因此，即使能够分析UbiComp结构的工具的设计仍然对研究人员提出了一些挑战，但我们可以乐观地展望未来。

**长期安全**

各种UbiComp系统被设计成可以承受很多年甚至几十年的寿命[54，55]。例如，在关键基础设施方面的系统往往需要在实地设计和部署大量的财政投资[56]，因此，如果这些系统在较长时间内继续使用，将提供更好的投资回报。汽车领域是一个特别感兴趣的领域。预计几十年内车辆都是可靠的[57]，更新车队或更新功能（召回）会增加车主的成本。请注意，现代车辆是育碧生态系统的一部分，因为它们配备了具有互联网连接的嵌入式设备。在未来，预计车辆将更多地依赖于通过无线技术在其他车辆/基础设施之间收集和共享的数据[58]，以便实现丰富的驾驶体验，如自主驾驶[59]。

还值得一提的是，设计为能承受数年或数十年寿命的系统可能会因缺乏未来维护而受到影响。有创新能力的公司之间的竞争非常激烈，导致公司在几年内倒闭的比率很高[60]。如果没有适当的维护，设备泛滥将给未来带来严重的挑战[61]。

从前面提到的几个例子中可以看出，越来越需要UbiComp系统在更长的时间内保持可靠，并且只要有可能，就需要尽可能少的更新。这些要求对此类系统的安全特性有直接影响：相对而言，它们提供的修补最终安全漏洞的机会比传统系统要少。鉴于在设计和利用新的安全漏洞方面取得了紧张和动态的进展，这是一个危急的局势。因此，从设计UbiComp系统的早期阶段就认识到确保长期安全所面临的科学挑战，而不是事后采取缓和措施，这一点至关重要。

**作为核心组件的密码学**

确保长期安全对于任何系统来说都是一项非常具有挑战性的任务，不仅仅是对于UbiComp系统。它至少要求每一个安全组件都能自己和连接到其他组件时都是经得起未来考验的。为了简化这个过大的攻击面，并且仍然能够提供有用的建议，我们将把注意力集中在大多数安全机制的主要组成部分上，如第4节所强调的，即密码学。

密码技术有多种类型。最传统的方法依赖于计算问题的硬度，例如整数分解[62]和离散对数问题[63，64]。目前的密码分析技术和现有的技术资源都认为这些问题是难以解决的。正因为如此，密码学家才能够基于这样的计算问题建立密码系统的安全实例。然而，由于各种原因（将在以下各节讨论），这类计划的未来证明条件岌岌可危。

**经典密码分析的进展**

任何密码系统未来证明条件的第一个威胁是指在密码分析方面的潜在进展，即旨在以比最初预测的更有效的方式（用更少的处理时间、内存等）解决底层安全问题的技术。广泛部署的方案有一个长期的学术和工业审查轨道，因此人们预计在针对此类方案的密码分析技术方面几乎没有进展。然而，最近的文献显示了一些有趣和出乎意料的结果，这可能暗示了相反的情况。

例如，在[65]中，Barbulescu等人。介绍了一种新的拟多项式算法来求解有限域小特征离散对数问题。离散对数问题是Diffie-Hellman密钥交换[66]、数字签名算法[67]及其椭圆曲线变体（分别为ECDH[68]和ECDSA[67]）的潜在安全问题，仅举几个广泛部署的密码系统。此密码分析结果仅限于具有小特征的有限域，这是攻击上述方案的实际实现的一个重要限制。然而，任何解决一个长期问题的次指数算法都应该被视为一个相关的迹象，表明密码分析文献可能仍然会有最终的突破。

设计具有长期安全性的UbiComp系统的架构师应该考虑这种情况。与固定的、单密钥大小的支持相比，支持各种（即比通常更高）安全级别的实现是首选的。对于方案中以某种方式影响其整体安全性的其他数量，应使用与密钥相同的方法。通过这种方式，UbiComp系统将能够有意识地适应未来的密码分析进展，或者至少降低安全升级的成本。

**量子攻击造成的未来破坏**

例如，Lov K. Grover 引入了一个量子算法 [[71](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR71" \o "Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of ACM STOC 1996. New York: ACM: 1996. p. 212–19.)] ，能够在函数（大小N）的域中找到一个元素，该元素具有高概率，仅导致输出只需O（N）步骤。该算法可用于加快对称加密的密码分析。例如，n位密钥的块密码只能为量子对手提供n/2 位的安全性。哈希函数将受依赖于预期安全属性的方式受到影响。在更详细信息中，n位摘要的哈希函数仅提供n/ 3 位针对冲突攻击的安全性和n/2 位针对图像前攻击的安全性。表[1](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Tab1)总结了这一评估。在这种情况下，AES-128 和 SHA-256（抗碰撞性）将无法满足 128 位（量子安全性）的最低可接受安全级别。请注意，如果使用较长的键和摘要大小，则块密码和哈希函数结构仍将保持安全。但是，这将导致重要的性能挑战。例如，AES-256 的效率比 AES-128 低 40%（由于 14 轮，而不是 10 轮）。

甚至比对称密码更为关键的是，量子计算机将提供指数级的加速来攻击大多数广泛部署的公钥密码系统。这是由于Peter Shor的算法[72]能够有效地分解大整数，并在多项式时间内计算大组元素的离散对数。这项工作的影响将是破坏性的RSA和基于ECC的方案，因为增加密钥大小是不够的：他们将需要完全取代。

在抗量子攻击的公钥密码系统领域，即能够抵抗量子攻击的替代公钥方案中，需要解决几个挑战。第一种是在学术界和工业界就如何战胜量子攻击达成共识。特别是，有两种被认为能够抵御量子攻击的主要技术，即：后量子密码（PQC）和量子密码（QC）。前者基于不同的计算问题，人们认为这些问题非常困难，甚至连量子计算机都无法解决。PQC方案的一个重要好处是，它们可以在当前可用的计算机中实现和部署[73–77]。后者（QC）依赖于量子基础设施的存在和部署，并且仅限于密钥交换目的[78]。部署量子基础设施的有限能力和非常高的成本最终应该导致对后量子密码技术趋势的共识。

文献中提供了几种PQC方案。例如，基于散列的签名（HBS）是最受认可的数字签名解决方案。最现代的结构[76，77]代表了Merkle签名方案的改进[74]。HBS的一个重要好处是，它们的安全性完全依赖于hash函数的某些已知属性（因此，假设使用了适当的摘要大小，它们就可以安全地抵御量子攻击）。关于其他安全特性，如密钥交换和非对称加密，学术界和工业界尚未达成共识，尽管基于代码和基于格的密码学文献已经提出了有希望的方案[79-85]。基于Isogeny的密码学[86]是一种较新的方法，具有一定的实用价值（例如相当小的公钥大小[87，88]），尽管它刚刚开始从对其密码分析属性的更全面的理解中获益[89]。关于标准化工作，NIST最近开始了后量子密码方案的标准化过程[90]，这至少需要几年时间才能得出结论。目前缺乏标准是一项重要挑战。特别是，未来可能会出现互操作性问题。

最后，后量子公钥密码系统中的另一个挑战是潜在的新实现要求或约束。如前所述，基于散列的签名是非常有前途的后量子候选者（考虑到与散列函数相关的效率和安全性），但也导致了一组新的实现挑战，例如保持方案状态安全的任务。更详细地说，大多数HBS方案都有随时间演变的私钥（它们的状态）。如果没有严格的状态管理策略，签名者可以重复使用同一个私钥两次，这将使方案提供的安全保证失效。最近，解决这些新的实现挑战的初步工作已经出现在文献中[91]。最近引入的HBS结构[92]展示了如何以更大的签名为代价摆脱国家管理问题。这些例子表明了PQC方案潜在的新的实现挑战，必须由UbiComp系统架构师解决。

**密码工程**

UbiComp系统涉及不同性质的构建块：硬件组件，如传感器和执行器，实现通信协议和与云提供商接口的嵌入式软件，以及最终的操作程序和其他人为因素。因此，普及系统有一个很大的攻击面，必须使用多种技术的组合来保护。

密码学是任何现代计算系统的基本组成部分，但不太可能是其攻击面中最弱的部分。网络协议、输入解析例程甚至带有加密机制的接口代码都是更容易受到攻击的组件。然而，由于风险集中在密码原语中，对密码安全属性的成功攻击通常是灾难性的。例如，违反机密性可能导致涉及敏感信息的大量数据泄露。对通信完整性的对抗性干扰可能允许偏离指定行为的命令注入攻击。可用性对于保持合法用户可以访问系统和保证持续的服务提供至关重要，因此加密机制也必须是轻量级的，以最大限度地减少攻击者滥用的可能性。

在UbiComp系统中部署密码学时，敌方对攻击面部分的物理访问是一个特别具有挑战性的方面。通过假设，对手可以恢复长期的秘密和凭证，从而对系统的一部分（希望是一小部分）提供某种控制。下面我们将探讨在为普及系统部署加密机制方面的一些主要挑战，包括如何管理密钥和实现高效和安全的加密实现。

**密钥管理**

根据定义，UbiComp系统是异构平台，连接具有巨大不同计算和存储能力的设备。为任何异构系统设计加密体系结构都需要为系统中每个实体负责的任务分配明确定义的角色和相应的安全属性。资源受限的设备应该接收较少的计算密集型任务，并且它们缺乏防篡改保护，这表明长期机密不应该存在于这些设备中。更重要的任务涉及昂贵的公钥加密，应该委派给更强大的节点。安全属性、功能性和加密原语之间的仔细权衡必须针对每台设备或每类设备[93]，遵循一套普适系统的指导原则：

* 功能：密钥管理协议必须管理加密密钥的生存期并确保当前授权用户的可访问性，但单独处理密钥管理和授权可能会增加复杂性和漏洞。将这两种服务组合到加密强制访问控制框架中的一种有希望的方法是基于属性的加密[94，95]，其中密钥具有一组功能和属性，可以根据需要进行授权和撤销。
* 通信：组件应尽量减少通信量，如果通信中断，则有无法操作的风险。这里推荐了密钥分配的非交互式方法[96]，但是由于解决离散对数问题的最新进展（在所谓的中素数情形[97]），基于双线性对的高级协议应该避免。这些进展有力地增加了参数的大小，降低了性能/可伸缩性，并可能进一步改进，有利于更传统的非对称加密形式。
* 效率：协议应该是轻量级的，易于实现，要求传统的公钥基础设施（pki）和昂贵的证书处理操作仅限于体系结构中功能更强大和连接更紧密的节点。支持隐式认证的替代模型包括基于身份的[98]（IBC）和无证书加密[99]（CLPKC），前者意味着固有的密钥托管。尽管取得了进展，但关键性撤销的困难仍然给它们的广泛采用设置了障碍[100]。基于高效密钥交换协议和隐式证书的轻量级配对和无托管认证密钥协议结合了这两种方法的优点，在节省带宽的同时提供了高性能[101]。
* 互操作性：普适系统由来自不同制造商的组件组成。支持跨域认证和授权框架对于互操作性至关重要[102]。

然后，参与联合功能的加密原语必须与所有端点兼容，并尊重功能较弱的设备的约束。

**轻量级密码**

UbiComp中大量互连设备的出现，推动了在轻量级密码体制下发展新的密码原语。轻量级并不意味着弱加密，而是应用定制的加密，特别是在资源消耗方面，如处理器周期、能量和内存占用方面，设计为高效的加密[103]。轻量级设计的目标是针对密码学的常见安全需求，但可能采用较不保守的选择或较新的构建块。

作为第一个例子，许多新的分组密码被提出作为高级加密标准（AES）的轻量级替代品[104]。重要的构造是LS设计[105]、现代ARX和Feistel网络[106]和替换置换网络[107108]。一个值得注意的候选者是目前的分组密码，它具有10年的抗密码分析尝试的成熟度[109]，并且其性能最近在软件领域变得有竞争力[110]。

在散列函数的情况下，为了在某些情况下简单起见，设计甚至可以权衡高级安全属性（如抗冲突性）。一个明显的例子是从非冲突的哈希函数（如SipHash[111]中）构造短消息认证码（MAC），或者从短输入哈希函数[112]构造数字签名。在传统应用中，BLAKE2[113]比最近发布的SHA-3标准[115]在软件方面的速度更快，取代了最近加密分析的标准[114]。

另一个趋势是通过使用关联数据 （AEAD） 进行身份验证加密，在单个步骤中提供机密性和身份验证。这可以通过块密码操作模式（如 GCM [[116](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR116" \o "McGrew DA, Viega J. The security and performance of the galois/counter mode (GCM) of operation. In: INDOCRYPT. LNCS, 3348 vol.Berlin: Springer: 2004. p. 343–55.)]）或专用设计实现。CAESAR 竞赛[脚注 1](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fn1) 选择新的 AEAD 算法，用于跨多个用例进行标准化，例如轻量级和高性能应用程序以及纵深防御设置。NIST 已经跟进并启动了自己的轻量级 AEAD 算法和哈希函数的标准化流程。

在公钥加密方面，Elliptic 曲线加密（ECC）[[63，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR63" \o "Miller VS. Use of elliptic curves in cryptography. In: CRYPTO, volume 218 of Lecture Notes in Computer Science. Berlin: Springer: 1985. p. 417–26.)[117](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR117" \o "Koblitz N. A family of jacobians suitable for discrete log cryptosystems. In: CRYPTO, volume 403 of LNCS. Berlin: Springer: 1988. p. 94–99.)]仍然是空间中反对基于保理的加密系统[[62](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR62" \o "Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978; 21(2):120–6.)]的主要竞争者， 因为一个潜在的问题推测在经典计算机中是完全指数。ECC的现代实例化具有高性能和实现简单性，非常适合嵌入式系统 [[118](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR118" \o "Bernstein DJ. Curve25519: New diffie-hellman speed records. In: Public Key Cryptography. LNCS, 3958 vol.Berlin: Springer: 2006. p. 207–28.),[120](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR120" \o )]。然而，数字理论基元的统治地位受到量子计算机的威胁，如第[3](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec6)节所述。

大量的新基元必须从安全性和性能的角度进行严格评估，同时涉及理论工作和工程方面。在不断减少的设备和更具侵入性的攻击下，实现预期会消耗更少的能量 [[121](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR121" \o "Banik S, Bogdanov A, Regazzoni F. Exploring energy efficiency of lightweight block ciphers. In: SAC. LNCS, 9566 vol.Berlin: Springer: 2015. p. 178–94.)]、周期和内存 [[122]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR122" \o "Dinu D, Corre YL, Khovratovich D, Perrin L, Großschädl J, Biryukov A. Triathlon of lightweight block ciphers for the internet of things. NIST Workshop on Lightweight Cryptography. 2015.)

**侧通道电阻**

如果实施时小心谨慎，否则安全加密算法或协议可能会泄漏可能对攻击者有用的重要信息。侧通道攻击 [[123](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR123" \o "Kocher PC. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In: CRYPTO. LNCS, 1109 vol.Berlin: Springer: 1996. p. 104–13.)] 是加密学的重大威胁，可能使用计时信息、缓存延迟、电源和电磁辐射来恢复机密材料。这些攻击产生于实现和底层计算机体系结构之间的交互，是普遍计算环境的一个内在安全问题，因为攻击者被假定至少对某些合法设备具有物理访问权限。

防范侵入式侧通道攻击是一个具有挑战性的研究问题，对策通常会促进计算的某种程度的*规律性*。在内存层次结构中执行时间差异或延迟的情况下，*等时*或恒定时间实现是解决此问题的第一批策略之一。正式方法的应用使第一个工具能够验证实现的等量性，例如信息流分析 [[124]](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR124" \o "Rodrigues B, Pereira FMQ, Aranha DF. Sparse representation of implicit flows with applications to side-channel detection In: Zaks A, Hermenegildo MV, editors. Proceedings of the 25th International Conference on Compiler Construction, CC 2016, Barcelona, Spain, March 12-18, 2016. New York: ACM: 2016. p. 110–20.)和程序转换 [[125](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR125" \o "Almeida JB, Barbosa M, Barthe G, Dupressoir F, Emmi M. Verifying constant-time implementations. In: USENIX Security Symposium. Berkeley: USENIX Association: 2016. p. 53–70.)] 。

虽然最近有一种趋势来构建和标准化加密算法，具有一些嵌入式电阻，以抵御更简单的时序和功率分析攻击 [[105](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR105" \o "Grosso V, Leurent G, Standaert F-X, Varici K. Ls-designs: Bitslice encryption for efficient masked software implementations. In: FSE. LNCS, 8540 vol.Berlin: Springer: 2014. p. 18–37.)]，但更强大的攻击（如差分功率分析 [[126]](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR126" \o "Kocher PC, Jaffe J, Jun B. Differential power analysis. In: CRYPTO. LNCS, 1666 vol. Springer: 1999. p. 388–97.)或故障攻击 [[127]](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR127" \o "Biham E, Shamir A. Differential fault analysis of secret key cryptosystems. In: CRYPTO. LNCS, 1294 vol.Berlin: Springer: 1997. p. 513–25.)是很难防止或缓解的。故障注入成为一种更强大的攻击方法，它在软件[[128](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR128" \o "Kim Y, Daly R, Kim J, Fallin C, Lee J-H, Lee D, Wilkerson C, Lai K, Mutlu O. Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. In: ISCA. Washington, DC: IEEE Computer Society: 2014. p. 361–72.)] 中演示后。

屏蔽技术 [[129](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR129" \o "Ishai Y, Sahai A, Wagner D. Private circuits: Securing hardware against probing attacks. In: CRYPTO. LNCS, 2729 vol. Springer: 2003. p. 463–81.)] 经常被研究作为从秘密数据中分离泄漏信息的对策，但经常需要强大的熵源来实现其目标。随机性回收技术作为启发式方法非常有用，但对这些方法的正式安全分析是一个公开的问题 [[130](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR130" \o "Balasch J, Gierlichs B, Grosso V, Reparaz O, Standaert F-X. On the cost of lazy engineering for masked software implementations. In: CARDIS. LNCS, 8968 vol.Berlin: Springer: 2014. p. 64–81.)] 。在基础体系结构中，在指令集扩展、简化的执行环境和事务机制方面进行修改以重新启动错误计算是另一个有前途的研究方向，但可能涉及对当前硬件的激进且可能成本高昂的更改。

**弹性**

UbiComp 依赖于连接、路由和端到端通信等基本服务。这些基本服务的进步使得Weiser的无处不在应用成为可能，它可以依靠透明的通信，同时满足最终用户在日常活动中的期望和要求。在用户的期望和要求中，服务的可用性（不仅是通信服务，而且由 UbiComp 提供给用户的所有服务）至关重要。越来越多的用户期望并支付全天候可用服务的费用。当我们考虑关键的 UbiComp 系统（例如与医疗保健、紧急性和车辆嵌入式系统相关的系统）时，这一点就更加相关。

本文强调了复原力，因为它是安全的支柱之一。复原力旨在识别、预防、检测和应对因服务不可用而造成的损失或技术故障，以恢复或减轻损害和经济损失[[131]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR131" \o "Nogueira M, dos Santos AL, Pujolle G. A survey of survivability in mobile ad hoc networks. IEEE Commun Surv Tutor. 2009; 11(1):66–77.)一般来说，服务不可用与非故意故障有关，但是，越来越多的故意利用服务可用性违规正在变得破坏性和失控，如最新的分布式拒绝服务 （DDoS） 攻击公司 DYN，一个领先的 DNS 提供商，以及DDoS攻击公司OVH，法国网站托管巨头 [[132，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR132" \o "Mansfield-Devine S. The growth and evolution of ddos. Netw Secur. 2015; 2015(10):13–20.) [133](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR133" \o )] 。后者的恶意流量约为 1 TB/s，这些流量来自大量地理分布和受感染的设备，如打印机、IP 摄像机、住宅网关和婴儿监视器。这些设备与UbiComp系统[[134]](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR134" \o )的现代概念直接相关，它们打算为用户提供无处不在的服务。

然而，这里最吸引注意力的是无处不在的利用对服务可用性的负面影响。事实是，马克·威瑟关于*21世纪计算机*的想法为新型高度破坏性的攻击打开了大门。这些攻击一般基于我们家庭、工程、城市和国家中的设备隐身和不知情的想法。但是，正因为如此，人们似乎没有充分重视基本做法，如在闭路电视摄像机、婴儿监视器、智能电视等互联网连接设备中更改默认密码。这一简单事实被指为前面提到的两次 DDoS 攻击的主要原因，全球专业服务公司德勤（Deloitte）的一份报告指出，分布式拒绝服务 （DDoS） 攻击在 2017 年会危及服务可用性，其规模和规模在 2017 年有所增加，部分原因是连接事物的多宇宙性日益增强。他们还提到 DDoS 攻击将更加频繁，估计几个月内将有 1000 万次攻击。

由于无法保证完全避免这些攻击，弹性解决方案成为减轻损害和快速恢复服务可用性的一种方式。然后，弹性是必要的，并且与我们在本文前几节中观察到的其他解决方案相辅相成。因此，本节重点强调在 UbiComp 系统中恢复能力的重要性。我们概述了 UbiComp 系统中关于弹性的最先进的技术，并指明了未来研究和创新的方向 [[135](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR135" \o "Santos AA, Nogueira M, Moura JMF. A stochastic adaptive model to explore mobile botnet dynamics. IEEE Commun Lett. 2017; 21(4):753–6.)，[138](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR138" \o "Lipa N, Mannes E, Santos A, Nogueira M. Firefly-inspired and robust time synchronization for cognitive radio ad hoc networks. Comput Commun. 2015; 66:36–44.)]。我们还理解，这些系统的复原力仍需要大量的调查，但我们认为，通过本文提出这一点进行讨论是我们的职责。

为了将适应力与 UbiComp 的情境结合，必须看到，信息和通信技术（如无线网络）的改进增加了分布式系统在日常生活中的使用。通过便携式设备和无线通信，网络访问变得无处不在，使人们越来越依赖它们。这增加了对同时高级别可靠性和可用性的依赖性。当前网络由异构便携式设备组成，它们之间通常以无线多跳方式进行通信 [[139](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR139" \o "Zhang C, Song Y, Fang Y. Modeling secure connectivity of self-organized wireless ad hoc networks. In: IEEE INFOCOM. Piscataway: IEEE: 2008. p. 251–5.)] 。这些无线网络可以自主适应其环境的变化，如设备位置、流量模式和干扰。每个设备都可以根据更改动态重新配置其拓扑、覆盖范围和信道分配。

由于当前网络的特点，例如共享无线介质、高度动态的网络拓扑、多跳通信和便携式设备的低物理保护[[140，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR140" \o "Salem NB, Hubaux J-P. Securing wireless mesh networks. IEEE Wirel Commun. 2006; 13(2):50–5.)[141]](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR141" \o "Yang H, Luo H, Ye F, Lu S, Zhang L. Security in mobile ad hoc networks: challenges and solutions. IEEE Wirel Commun. 2004; 11(1):38–47.)，UbiComp 对弹性设计提出了非同寻常的挑战。此外，不同方案中缺少中央实体会增加弹性管理的复杂性，尤其是当它与访问控制、节点身份验证和加密密钥分发相关联时。

网络特征，以及针对破坏服务可用性的攻击的其他解决方案的限制，强化了这样一个事实，即没有一个网络能够完全不受攻击和入侵的影响。因此，需要采用新的方法来促进网络服务的可用性。这些要求促使弹性网络服务的设计。在这项工作中，我们专注于将数据从一个UbiComp设备传递到另一个UbiComp设备作为基本网络功能，并强调三项基本服务：物理和链路层连接、路由和端到端逻辑通信。然而，在其他角度也观察到复原力。我们遵循这样的主张：在跨层安全解决方案上实现弹性，该解决方案以自自适应和协调的方式集成了预防性（即加密和访问控制）、反应性（即入侵检测系统）和容错（即数据包冗余）防御线[[131，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR131" \o "Nogueira M, dos Santos AL, Pujolle G. A survey of survivability in mobile ad hoc networks. IEEE Commun Surv Tutor. 2009; 11(1):66–77.)[142](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR142" \o "Nogueira M. SAMNAR: A survivable architecture for wireless self-organizing networks. PhD thesis, Université Pierre et Marie Curie - LIP6. 2009.)]。

然而，在UbiComp背景下实现复原力的公开挑战是什么？首先，我们强调组成UbiComp环境的设备和技术的异质性。从大型系统（如云数据中心）到可穿戴和可植入传感器等微型设备的集成本身是一个巨大的挑战，因为它的复杂性。此外，面对这些设备的不同要求、其内存和处理能力以及应用，提供预防性、反应性和耐受性解决方案的集成及其适应就更加困难了要求。此外，处理通信技术和协议方面的异质性使得对网络行为和拓扑的分析具有挑战性，传统系统中使用哪些技术来帮助设计弹性解决方案。

另一个挑战是如何处理规模问题。首先，UbiComp 系统往往是超大规模和地理分布的。那么，如何应对由此带来的复杂性呢？如何定义和构建模型来理解这些系统并提供弹性服务？最后，我们还指出，作为挑战的不确定性和速度。如果一方面，在这个复杂的系统中，很难对弹性服务进行建模、分析和定义，另一方面，不确定是这些服务的常态，即速度和响应时间低是这些系统中应用的强烈要求。因此，如何共同解决所有这些要素？如何管理它们，以便根据各种应用程序的不同要求提供弹性服务？

所有这些问题都会导致深入的调查和挑战。然而，它们也显示了在设计和工程弹性系统中的应用研究机会，主要是针对UbiComp上下文。特别是，如果我们提倡设计弹性系统，以自适应的方式管理三道防线。我们相信，这种管理可以促进应用研究和复原力的巨大进步。

**隐私影响**

UbiComp系统倾向于收集大量数据并生成大量信息。信息使用得当，为我们的社会带来了无数的利益，多年来，信息为我们提供了更好的生活。但是，这些信息可用于非法目的，就像计算机系统用于攻击一样。保护私人信息是一项巨大的挑战，通常看起来不切实际，例如，保护客户的电力消耗数据免受配电公司[[184](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR184" \o "Borges F, Demirel D, Bock L, Buchmann JA, Mühlhäuser M. A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In: ISCC. USA: IEEE: 2014. p. 1–6.)–[186](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR186" \o "Borges de Oliveira F. Reasons to Measure Frequently and Their Requirements. Cham: Springer International Publishing; 2017. p. 39–47.)]的利用）。

确保安全是确保隐私的必要条件，例如，如果客户端和服务提供商之间的通信不安全，则隐私得不到保障。但是，它不是一个足够的条件，例如，通信是安全的，但服务提供商以不允许的方式使用数据。我们可以使用加密技术来确保安全和隐私。但是，即使使用加密通信，网络流量中的元数据也可能显示私人信息。第一个挑战是找出数据相关性的扩展和数据泄漏的影响。

**应用程序方案挑战**

查找哪些数据可能敏感是一项具有挑战性的任务。当某些区域性将相同的数据归类为公共数据时，某些区域性将某些数据分类为敏感数据。另一个挑战是处理来自不同国家的法规。

**识别敏感数据**

对可能敏感的数据进行分类可能是一项具有挑战性的任务。联合国大会1948年12月10日在巴黎宣布的《世界人权宣言》第12条规定：任何人不得任意干涉其隐私、家庭、家庭或通信，不得侵犯其名誉和名誉。人人有权受到法律保护，免受这种干涉或攻击。立法者已经改进了世界各地的隐私法。然而，仍然有很大的改进空间，特别是当我们考虑来自人、动物和产品的数据时。提供商可以使用此类数据来分析并操纵人员和市场。不公平的竞争对手可能会利用私人工业数据来获得相对于其他行业的优势。

**调节**

UbiComp 系统倾向于在全球运行。因此，他们的开发人员需要处理来自不同文化的若干法律。法律的丰富对国际机构来说是一个挑战。缺乏法律。一方面，法律的过激迫使机构处理庞大的官僚机构，以遵循几项法律。另一方面，缺乏法律会导致不公平竞争，因为不道德的公司可以利用私人数据来获得优于道德公司的优势。商业模式必须使用隐私保护协议来确保民主，避免出现监视社会（见[[187]）。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR187" \o "Holvast J. The Future of Identity in the Information Society, volume 298 of IFIP Advances in Information and Communication Technology In: Matyáš V, Fischer-Hübner S, Cvrček D, Švenda P, editors. Berlin: Springer Berlin Heidelberg: 2009. p. 13–42.)此类协议是解决隐私和信息之间两难困境的解决方案。然而，它们有自己的技术挑战。

**技术挑战**

我们可以处理从旧系统收集的已收集的数据或由隐私保护协议收集的私有设计数据，例如，旧系统中使用的数据库和来自隐私保护协议的消息。如果一个场景可以归为两者，我们可以在短期内将其作为已收集的数据处理。

**已收集的数据**

可以使用数据集进行信息检索，同时保持真实所有者数据的匿名性。在私有数据集上可以使用数据挖掘技术。在隐私保护数据挖掘中使用了几种技术[[188](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR188" \o "Toshniwal D. Privacy preserving data mining techniques privacy preserving data mining techniques for hiding sensitive data hiding sensitive data: a step towards open data open data. Singapore: Springer Singapore: 2018. p. 205–12.)]。ARX 数据匿名工具是一个非常有趣的工具，用于对已经收集的数据进行匿名化。在下面，我们介绍了几种用于在已收集的数据中提供隐私的技术。

**匿名化**

目前，我们有几种匿名化技术，用于评估匿名化水平，例如，k- 匿名、l-多样性和t-接近性 [[189](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR189" \o "Li N, Li T, Venkatasubramanian S. t-closeness: Privacy beyond k-anonymity and l-diversity. In: 2007 IEEE 23rd International Conference on Data Engineering. USA: IEEE: 2007. p. 106–15.)]。它们使用表中无法区分的标识符的集E。

方法k-匿名性禁止显示表列或替换表列，以便使每个E具有至少k寄存器。这似乎是安全的，但只有4点标记在时间上的位置足以识别唯一95%的手机用户[[190]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR190" \o "De Montjoye Y-A, Hidalgo CA, Verleysen M, Blondel VD. Unique in the crowd: The privacy bounds of human mobility. Sci Rep. 2013; 3:1–5.)

方法l- 多样性要求每个E具有每个敏感列的至少l值"良好表示"。良好表示方式可通过三种方式定义：

1. 每个敏感列至少l个不同的值;

2.对于每个E，香农熵是有限的，像这样H(E)≥log2L，其中 H(E)=−∑s∈SPr(E,s)log2(Pr(E,s))，S是敏感列的域，Pr（E，s）是E中具有敏感值的线的概率;

3. 最常见的值不能频繁出现，最不常见的值不能不常出现。

请注意，某些表没有l不同的敏感值。此外，表熵应至少为对2l。此外，公共值和非命令值的频率通常并不接近。

我们说，如果敏感列E的分布距离结束所有表中列的分布不超过阈值t，则E是t-接近性。因此，我们说，如果表中的每个E具有t-紧密性，则表具有t-接近性。在这种情况下，该方法会在数据有用性和隐私之间产生权衡。

**差别隐私**

差异隐私的概念与密码学中的不可区分性概念类似。要定义它，让*ε* 成为正实数， A是一种概率算法，数据集作为输入。我们说 A 是私有的*ε*-differentially，如果对于每个数据集D1 和D2 在一个元素中不同，并且对于A图像的每个子集S我们有公式 ，其中算法随机性控制概率。

差异隐私不是数学意义上的指标。但是，如果算法基于输入保持概率，我们可以构造一个指标d来比较两个算法之间的距离通过方式d(A1,A2)=|ϵ1−ϵ2|.d(A1,A2)=|ϵ1−ϵ2|，我们可以确定两个算法是否等效ε1=ε2，我们可以确定与理想算法计算的距离 d(A1,Aideal)=|ϵ1−0|

熵和匿名程度

匿名程度g可以使用香农熵测量公式2， 其中H（X） 是网络熵，N是节点数，pi是每个节点i的概率。当概率是均匀的，即所有节点都相等 1/N时，就会发生最大熵，因此HM• log2（N）。因此，匿名度g的定义是

公式3

与差异隐私类似，我们可以构造一个指标来比较两个网络计算d（g）之间的距离d(g1,g2)=|g1−g2|。同样，我们可以比较，如果他们是等效的g1•g2.因此，我们可以确定与理想匿名网络计算的距离d(g1,gideal)=|g1-1|。

网络可以替换为数据集，但在此模型中，每个寄存器都应具有概率。

**复杂性**

复杂性分析还可用作度量度量从匿名数据集检索信息的最佳情况下所需的时间。它也可以在私有设计数据中使用，作为破坏隐私保护协议所需的时间。时间度量可以通过不温而久算分析或计算破坏方法的步骤数来完成。

所有技术都有其优点和缺点。但是，即使复杂性防止泄漏，即使算法具有不同的隐私，即使匿名程度是最大，隐私也可能遭到侵犯。例如，在有3个选民的选举中，如果2个相互勾结，那么第三个选民的隐私将不受使用算法的影响。在[[191](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR191" \o "Borges de Oliveira F. Quantifying the aggregation size. Cham: Springer International Publishing; 2017. p. 49–60.)]中，我们发现如何打破基于智能电网噪声的协议，即使它们具有差分隐私的属性。

加密应确保隐私，确保安全性。加密邮件应具有最大的隐私指标以及加密确保的安全性。我们应该使用泄漏隐私并计算其最坏情况复杂性的最佳算法。

**概率**

我们可以使用概率来测量泄漏的可能性。此方法与用于保护隐私的算法无关。

例如，考虑有 3 名选民的选举。如果 2 个选民投"是"，1 个选民投否，攻击者知道选民投"是"的概率为 2/3，否的概率为 1/3。如果选民和候选人的数量增加，同样的逻辑也适用。

与"是"和"否"的情况不同，我们可能不让隐私受到重视。为了让攻击者发现第三个点的时间序列，它们将每个点表示为多个星，即符号\*。因此，攻击者可以将星的总数分成三个框。假设级数的总和为7，则概率为\*\*\*\* \* \*\*。为简单起见，攻击者可以按条形而不是框将星形拆分。因此，\*\*\*\*|\*|\*\*是相同的解决方案。用这样的符号，7 星的二项式加上两条选择的7星决定了可能的解的数目，即

公式4

一般来说，如果t是时间序列中的点数及其和，那么攻击者判断正确的可能时间序列的数目由s加t-1选择的s决定，即

公式5 (1)

如果我们收集多个时间序列，我们可以形成一个表，例如，按州投票次数的候选人名单。计票员冷只显示选民总数按州和候选人的总数，谁可以推断可能的投票数由州[[191](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR191" \o "Borges de Oliveira F. Quantifying the aggregation size. Cham: Springer International Publishing; 2017. p. 49–60.)]。以往选举的数据可能有助于估计。与*匿名、l-*多样性和*t-close*的匿名化相比，通过加密数据计算选举结果要安全得多。不过，根据表的大小及其值，可以找到时间序列。

通常，我们可以考虑测量而不是值。匿名技术试图减少表中的测量次数。与直觉相反，测量次数减少，发现它们的几率更大 [[191](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR191" \o "Borges de Oliveira F. Quantifying the aggregation size. Cham: Springer International Publishing; 2017. p. 49–60.)] 。

如果我们在设计上考虑隐私，我们尚未收集数据。

**私有设计数据**

消息是私有设计数据的常见词。消息被传输、处理和存储。对于隐私保护协议，不应泄露单个消息。克里普特布德是一个有趣的工具，它允许我们通过加密数据集进行查询。尽管消息存储在数据集中，但它们是使用用户密钥的加密消息。为了保持性能合理，隐私保护协议聚合或合并消息并解决特定问题。

**计算所有运算符**

理论上，我们可以通过加密数据计算都灵机器，即，我们可以使用一种称为完全同构加密[[192](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR192" \o "Gentry C. A Fully Homomorphic Encryption Scheme. Stanford: Stanford University; 2009. AAI3382729.)]的技术来计算任何通过加密数据运算符。完全同构加密的重大挑战是性能。因此，为许多应用程序方案构建完全同构加密是一项艰巨的任务。最常见的操作是添加。因此，大多数隐私保护协议使用加同态加密[[193](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR193" \o "Borges de Oliveira F. A Selective Review. Cham: Springer International Publishing; 2017. p. 25–36.)]和DC-Nets（来自"餐饮密码学家"）[[194](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR194" \o "Borges de Oliveira F. Selected Privacy-Preserving Protocols. Cham: Springer International Publishing; 2017. p. 61–100.)]。独立于操作，前者生成函数，后者生成函数系列。我们可以构建一个基于加构同态加密的不对称[DC-Net[194]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR194" \o "Borges de Oliveira F. Selected Privacy-Preserving Protocols. Cham: Springer International Publishing; 2017. p. 61–100.)

**强制执行和可塑性之间的权衡**

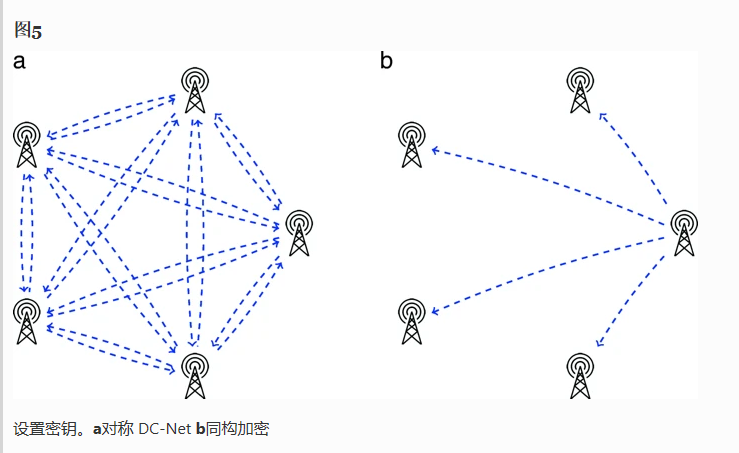
隐私强制成本很高。有了DC-Nets，我们可以强制保护隐私。但是，在计算中需要考虑每个加密消息，以便用户解密和访问协议输出。它有利于隐私，但不利于容错。举个例子，考虑所有选民都需要投票的选举。同构加密使协议能够解密和输出，甚至缺少加密的消息。实际上，它允许解密单个加密邮件。因此，同构加密无法确保隐私。为了说明这一点，考虑一个可以阅读和更改所有选票的选举。同构加密技术是可塑性的，DC-Nets 是不可塑性的。一方面，可邮寄性简化了流程，提高了容错能力，但禁用了隐私强制。另一方面，非邮件性会强制保护隐私，但会使过程复杂化，并降低容错能力。此外，同构加密的密钥分布比使用 DC-Net 方案更容易。

**密钥分发**

同构加密需要公钥对- 密钥对。谁拥有私钥控制所有信息。假设接收方生成密钥对，并将公钥发送到安全通信通道中的发送方。因此，发件人将使用相同的密钥来加密其邮件。由于同构加密方案是概率的，因此发送方可以使用同一密钥加密同一邮件，因为其加密邮件彼此不同。但是，接收方不知道谁发送了加密的消息。

DC-Net 需要每个用户的私钥和协议的公钥。由于 DC-Net 不需要发送方和接收方，因此用户通常被命名为参与者。它们生成自己的私钥。实际对称 DC-Nets 需要参与者在安全通信通道中相互发送密钥。之后，每个参与者都有一个由共享密钥列表给出的私钥。因此，每个参与者加密计算公式6， 其中*mi*，*j* 是参与者*i*在时间*j*中发送的消息，哈希是参与者预定义的安全哈希函数*，si,o*是从参与者*i*发送到参与者*o*的密钥，类似*地，so*，*i是i从* *o*接收的密钥 ，||是串联运算符。每个参与者*都可以*发送加密的消息 M*i*,*j* 对方。因此，参与者可以解密聚合的加密消息计算公式7. 请注意，如果缺少一个或多个消息，则解密是不可行的。非对称 DC-Net 不需要基于共享密钥的私钥。每个参与者只需生成一个私钥。随后，他们使用同构加密或对称 DC-Net 来添加生成解密密钥的私钥。

与 DC-Nets 相比，同构加密方案在设置密钥和分发密钥时具有较低的开销。对称直流网需要*O（I*2） 消息来设置密钥，其中*I*是参与者的数量。图[5](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig5)描述了使用 （a） 对称 DC-Net 和 （b） 同构加密设置密钥的消息。非对称DC-Nets比对称DC-Net更容易解决，其价格是信任同态加密方案。

**聚合和整合**

与同构加密相比，使用 DC-Nets 进行聚合和整合更容易。使用 DC-Nets，参与者只需广播其加密消息，或直接发送到聚合器。使用同构加密，发送方无法将加密邮件直接发送到接收方，收件人可以解密单个消息。不知何故，发送方应该聚合加密的消息，并且接收方应该只接收加密的聚合，这是同构加密的挑战，在DC-Nets中，由于[第7.4.2](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec34)节中描述的权衡，这是一项挑战。在这项工作中，我们将 DC-Nets 称为完全连接的 DC-Nets。对于未完全连接的 DC-Nets，聚合基于信任并产生新的挑战。有时，聚合和合并用作同义词。但是，与聚合相比，合并更为复杂，并生成更精细的信息。例如，加密文本消息的聚合只是为了联接它们，而加密文本消息的合并将生成语音合成。

**性能**

完全同构加密往往具有大密钥，并且需要令人望而却步的处理时间。相反，非对称DC-Nets和部分同构加密通常使用模块化多指数，可以用对数时间计算[[195]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR195" \o "Borges F, Lara P, Portugal R. Parallel algorithms for modular multi-exponentiation. Appl Math Comput. 2017; 292:406–16.)对称 DC-Nets 仅对少数参与者有效，因为每个参与者都需要对参与者数进行迭代以加密消息。参与者的数量与非对称DC-Nets和同态加密无关。

**取证**

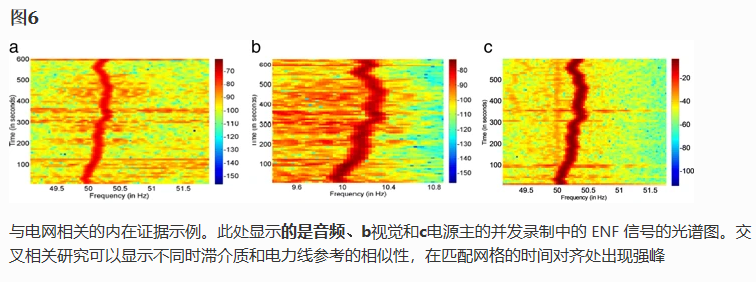
数字取证是法医学的一个分支，用于恢复和调查在数字设备中发现的材料。证据的收集和解释在法证中起着关键作用。传统的法医方法分别处理与计算机取证和信息取证有关的问题。然而，安全和法证研究的趋势日益明显，利用跨学科方法提供丰富的法证能力，以便利数据的认证以及访问条件，包括谁、何时、何地、以及如何。

在这种趋势中，有两种主要的法医证据类型[[196](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR196" \o "Stamm MC, Wu M, Liu KJR. Information forensics: An overview of the first decade. IEEE Access. 2013; 1:167–200.)]一种类型是设备、信息处理链或物理环境固有的，其形式包括与特定类型的硬件或软件处理或环境相关的特殊特征、作为特定设备单元特征的独特噪声模式、与特定设备相关的某些规律性或相关性、处理或其组合等。另一种类型是外在方法，即特别设计的数据主动注入信号/数据或物理世界中，然后提取和检查以推断或验证宿主数据的来源、完整性、处理历史记录或捕获环境。

在数字和物理系统与传感器、执行器和计算设备紧密相连的融合中，已提出一个新兴的框架，称为校对传感（PCS） [[197](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR197" \o "Wu M, Quintão Pereira FM, Liu J, Ramos HS, Alvim MS, Oliveira LB. New directions: Proof-carrying sensing — Towards real-world authentication in cyber-physical systems. In: Proceedings of ACM Conf. on Embedded Networked Sensor Systems (SenSys). New York: ACM: 2017.)] 。这灵感来自校对代码，这是一个受信任的计算框架，将外国可执行文件与模型关联，以证明它们未被篡改，并且按预期运行。在涉及移动和资源限制常见的网络物理系统的新 UbiComp 上下文中，物理世界可以用作一个通道，封装难以远程篡改的属性，如邻近性和因果关系，以创建挑战响应功能。这种校对传感框架可以帮助对设备、收集的数据和位置进行身份验证，与传统的多因素或带外身份验证机制相比，它具有独特的优势，即身份验证证明嵌入传感器数据中，无需运行复杂的加密算法即可在时间和空间上持续验证。

就上述内在和外在观点而言，在PCS框架中建立相互信任的可用物理数据可能是物理环境的内在数据（如温度、光度、噪声、电频率），或者例如，它们被设备主动注入到物理世界中。通过监控内部或外在数据的传播，设备可以确认其附近其他设备的接收情况。设计和安全实施此类协议的挑战可以通过信号处理、统计检测和学习、密码学、软件工程和电子学等综合专业知识的协同作用来解决。

为了帮助理解解决 UbiComp 中涉及数字和物理元素的安全性和取证的内在和外在证据，我们现在讨论两个示例。首先考虑电网的内在特征。电网频率 （ENF） 是配电网的供电频率，标称值为 60Hz（北美）或 50Hz（欧洲）。在任何给定时间，由于电网负载变化与发电控制机制之间的动态相互作用，ENF 的瞬时值通常围绕其标称值波动。由于网格的互连性质，这些变体在给定时间同一网格的所有位置几乎相同。瞬时 ENF 随时间的变化值形成 ENF 信号，该信号可以通过音频/视频记录（图[6）](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig6)或其他传感器（图 6 ）进行内在捕获[[198，](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR198" \o "Grigoras C. Applications of ENF analysis in forensic authentication of digital audio and video recordings. J Audio Eng Soc. 2009; 57(9):643–61.)[199](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR199" \o "Garg R, Varna AL, Hajj-Ahmad A, Wu M. \“seeing\” enf: Power-signature-based timestamp for digital multimedia via optical sensing and signal processing. TIFS. 2013; 8(9):1417–32.)]。这导致了最近的取证应用，例如验证包含ENF的多媒体信号的录制时间，并使用来自电网的并发参考信号根据ENF信号估计其记录位置。

 接下来，考虑萨奇达南丹和Kumar[[200]](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR200" \o "Satchidanandan B, Kumar PR. Dynamic watermarking: Active defense of networked cyber–physical systems. Proc IEEE. 2017; 105(2):219–40.)最近的作品，在网络物理系统中引入了水印的概念，它可以被视为一类外在特征签名。如果执行器向系统注入一个事先未知的正确设计的探测信号到系统中的其他节点，那么根据对网络物理系统动力学和其他属性的了解，执行器可以检查传感器关于不同点信号的报告，并可能推断系统中是否存在恶意活动，如果是，在何处以及如何。

一个重大挑战和研究机会在于发现和描述合适的内在和外在证据。尽管某些特征的定性特性是已知的，但开发定量模型来描述整个系统上下文中的正常和异常行为非常重要。沿着这条线，对物理模型的探索可能会产生这种属性的分析近似值;同时，数据驱动的学习方法可用于收集描述正常和异常行为的统计数据。基于这些要素，应开发跨越计算机取证、信息取证和设备取证等传统独立领域边界的强大协同作用，以实现系统取证的综合能力。

**结论**

用马克·威瑟的话说，无所不在的计算是"将计算机无缝地集成到整个世界的想法["[1]。](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR1" \o "Weiser M. The computer for the 21st century. Sci Am. 1991; 265(3):94–104.)因此，UbiComp系统的设计和实践早在四分之一世纪前就已经被讨论了，这远非当时的现象。在本文中，我们从安全和隐私的角度重新审视了这个贯穿我们社会最不同层次的概念。在未来几年里，这两个课题将占据研究人员和工程师的大部分时间。我们认为，利用这一时间应以以下几项意见为指导：

* UbiComp 软件通常作为不同编程语言的组合生成，共享一个通常以类型不安全的语言（如 C、C++ 或程序集）实现的共同核心。在此域中构建的应用程序倾向于分布式，其分析（即通过静态分析工具）需要考虑系统的整体视图。
* 其中一些系统的使用寿命长，加上更新和重新部署这些系统（包括操作和成本方面的困难），使它们容易受到技术和密码分析技术不可阻挡的进步的影响。这给这个讨论带来了新的（而且可能具有破坏性的）参与者，比如量子对手。
* 密钥管理是任何安全或私有真实系统的关键组件。在为框架中的所有实体明确定义安全角色和密钥管理过程后，必须部署一组匹配的加密基元。物理访问和受限资源使高效和安全的加密算法的设计复杂化，这些算法通常适合侧通道攻击。因此，目前空间的研究挑战包括更有效的钥匙管理计划，特别是支持某种形式的撤销;设计有助于正确和安全实现的轻量级加密基元;通过算法和嵌入式架构的进步提供了更便宜的侧通道电阻对策。
* 随着 UbiComp 系统的日益普及，人们越来越依赖他们的服务来执行不同的商业、金融、医疗和社会交易。这种日益增长的依赖性要求同时提供高水平的可靠性、可用性和安全性。这一观察加强了弹性UbiComp系统的设计和实施的重要性。
* 提供无处不在的 IdM 的主要挑战之一是确保具有多个异构安全域的方案中设备和用户以及自适应授权的真实性。
* 多个数据库当前存储敏感数据。此外，大量传感器不断收集新的敏感数据并将其存储在云中。正在设计和完善隐私保护协议，以在特定情况下增强用户的隐私。对隐私的文化解释、各种法律、云中遗留系统的大数据、处理时间、延迟、密钥分发和管理等，都是我们开发隐私保护协议的挑战。
* 物理系统和数字系统之间的融合在提供取证能力以促进数据认证以及访问条件（包括人员、何时、何地和如何）方面带来了挑战和机遇;将结合内在和外在证据与跨学科专业知识进行协同使用将是关键。

鉴于这些观察结果以及无所不在计算的重要性，我们很容易得出这样的结论：未来面临着令人着迷的挑战，等待学术界和业界的关注。

最后，请注意本作品中关于 UbiComp 如何演变的观察和预测，代表了基于当今技术前景的我们对该领域的看法。新的科学发现、技术发明以及经济、社会和政策因素可能导致技术进化路径中新的和/或不同的趋势。

**原文：**

**The computer for the 21st century: present security & privacy challenges**

[Journal of Internet Services and Applications](https://jisajournal.springeropen.com/) volume 9, Article number: 24 (2018)

**Abstract**

Decades went by since Mark Weiser published his influential work on the computer of the 21st century. Over the years, some of the UbiComp features presented in that paper have been gradually adopted by industry players in the technology market. While this technological evolution resulted in many benefits to our society, it has also posed, along the way, countless challenges that we have yet to surpass. In this paper, we address major challenges from areas that most afflict the UbiComp revolution:

1. Software Protection: weakly typed languages, polyglot software, and networked embedded systems.

2. Long-term Security: recent advances in cryptanalysis and quantum attacks.

3. Cryptography Engineering: lightweight cryptosystems and their secure implementation.

4. Resilience: issues related to service availability and the paramount role of resilience.

5. Privacy Implications: sensitivity data identification and regulation.

6. Forensics: trustworthy evidence from the synergy of digital and physical world.

We point out directions towards the solutions of those problems and claim that if we get all this right, we will turn the science fiction of UbiComp into science fact.

**Introduction**

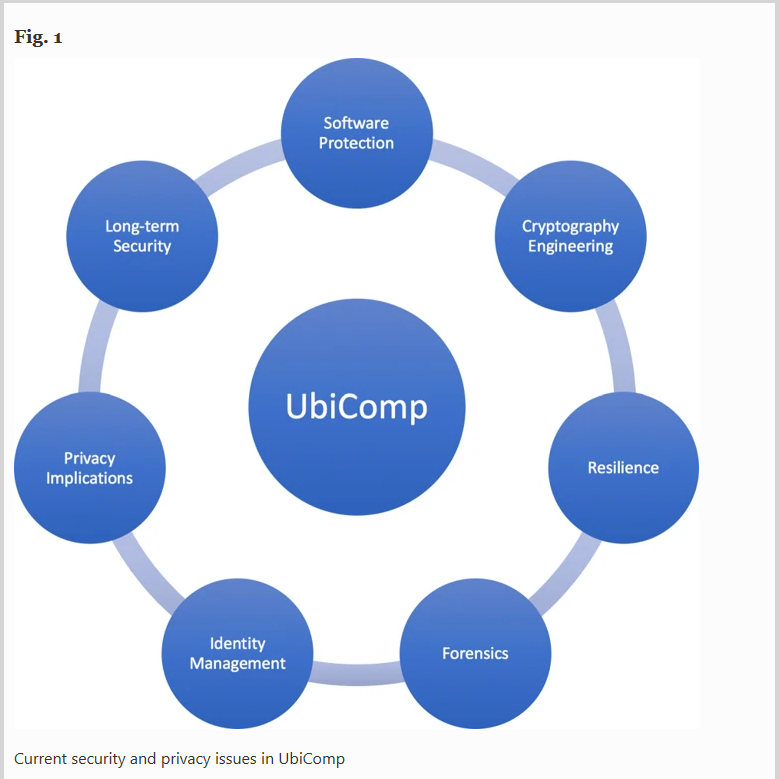
In 1991, Mark Weiser described a vision of the Computer for the 21st Century [[1](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR1" \o "Weiser M. The computer for the 21st century. Sci Am. 1991; 265(3):94–104.)]. Weiser, in his prophetic paper, argued the most far-reaching technologies are those that allow themselves to disappear, vanish into thin air. According to Weiser, this oblivion is a human – not a technological – phenomenon: “Whenever people learn something sufficiently well, they cease to be aware of it,” he claimed. This event is called “tacit dimension” or “compiling” and can be witnessed, for instance, when drivers react to street signs without consciously having to process the letters S-T-O-P [[1](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR1" \o "Weiser M. The computer for the 21st century. Sci Am. 1991; 265(3):94–104.)].

A quarter of a century later, however, Weiser’s dream is far from becoming true. Over the years, many of his concepts regarding pervasive and ubiquitous computing (UbiComp) [[2](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR2" \o "Weiser M. Some computer science issues in ubiquitous computing. Commun ACM. 1993; 36(7):75–84.), [3](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR3" \o "Lyytinen K, Yoo Y. Ubiquitous computing. Commun ACM. 2002; 45(12):63–96.)] have been materialized into what today we call Wireless Sensor Networks [[4](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR4" \o "Estrin D, Govindan R, Heidemann JS, Kumar S. Next century challenges: Scalable coordination in sensor networks. In: MobiCom’99. New York: ACM: 1999. p. 263–70.), [5](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR5" \o "Pottie GJ, Kaiser WJ. Wireless integrated network sensors. Commun ACM. 2000; 43(5):51–8.)], Internet of Things [[6](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR6" \o "Ashton K. That ’Internet of Things’ Thing. RFiD J. 2009; 22:97–114.), [7](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR7" \o "Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput Netw. 2010; 54(15):2787–805.)], Wearables [[8](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR8" \o "Mann S. Wearable computing: A first step toward personal imaging. Computer. 1997; 30(2):25–32.), [9](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR9" \o "Martin T, Healey J. 2006’s wearable computing advances and fashions. IEEE Pervasive Comput. 2007; 6(1):14–6.)], and Cyber-Physical Systems [[10](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR10" \o "Lee EA. Cyber-physical systems-are computing foundations adequate. In: NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, volume 2. Citeseer: 2006.), [11](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR11" \o "Rajkumar RR, Lee I, Sha L, Stankovic J. Cyber-physical systems: the next computing revolution. In: 47th Design Automation Conference. ACM: 2010.)]. The applications of these systems range from traffic accident and CO2 emission monitoring to autonomous automobile and patient in-home care. Nevertheless, besides all their benefits, the advent of those systems per se have also brought about some drawbacks. And, unless we address them appropriately, the continuity of Weiser’s prophecy will be at stake.

UbiComp poses new drawbacks because, vis-à-vis traditional computing, it exhibits an entirely different outlook [[12](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR12" \o "Abowd GD, Mynatt ED. Charting past, present, and future research in ubiquitous computing. ACM Trans Comput Human Interact (TOCHI). 2000; 7(1):29–58.)]. Computer systems in UbiComp, for instance, feature sensors, CPU, and actuators. Respectively, this means they can hear (or spy on) the user, process her/his data (and, possibly, find out something confidential about her/him), and respond to her/his actions (or, ultimately, expose she/he by revealing some secret). Those capabilities, in turn, make proposals for conventional computers ill-suited in the UbiComp setting and present new challenges.

In the above scenarios, some of the most critical challenges lie in the areas of Security and Privacy [[13](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR13" \o "Stajano F. Security for ubiquitous computing.Hoboken: Wiley; 2002.)]. This is so because the market and users often pursue a system full of features at the expense of proper operation and protection; although, conversely, as computing elements pervade our daily lives, the demand for stronger security schemes becomes greater than ever. Notably, there is a dire need for a secure mechanism able to encompass all aspects and manifestations of UbiComp, across time as well as space, and in a seamless and efficient manner.

In this paper, we discuss contemporary security and privacy issues in the context of UbiComp (Fig. [1](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig1)). We examine multiple research problems still open and point to promising approaches towards their solutions. More precisely, we investigate the following challenges and their ramifications.



1. Software protection in Section [2](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec2): we study the impact of the adoption of weakly typed languages by resource-constrained devices and discuss mechanisms to mitigate this impact. We go over techniques to validate polyglot software (i.e., software based on multiple programming languages), and revisit promising methods to analyze networked embedded systems.

2. Long-term security in Section [3](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec6): we examine the security of today’s widely used cryptosystems (e.g., RSA and ECC-based), present some of the latest threats (e.g., the advances in cryptanalysis and quantum attacks), and explore new directions and challenges to guarantee long-term security in the UbiComp setting.

3. Cryptography engineering in Section [4](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec10): we restate the essential role of cryptography in safeguarding computers, discuss the status quo of lightweight cryptosystems and their secure implementation, and highlight challenges in key management protocols.

4. Resilience in Section [5](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec14): we highlight issues related to service availability and we reinforce the importance of resilience in the context of UbiComp.

5. Privacy implications in Section 6: we explain why security is necessary but not sufficient to ensure privacy, go over important privacy-related issues (e.g., sensitivity data identification and regulation), and discuss some tools of the trade to fix those (e.g., privacy-preserving protocols based on homomorphic encryption).

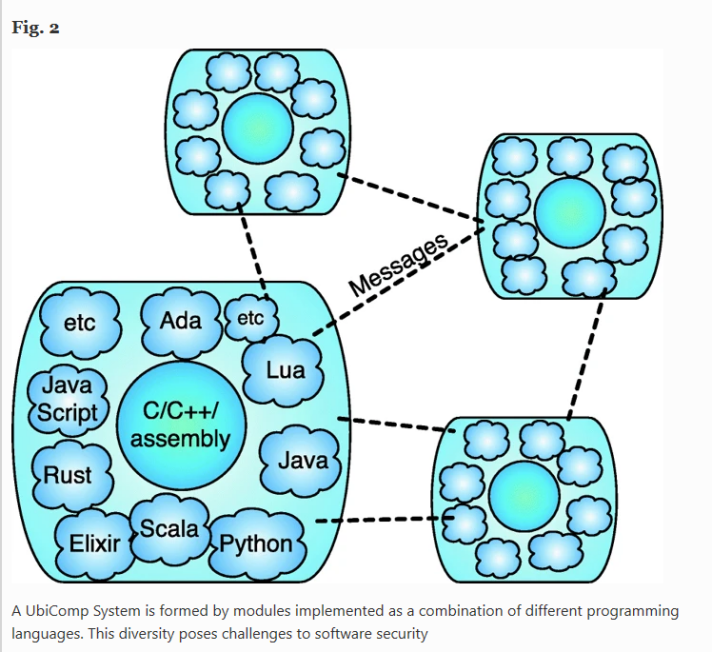
6. Forensics in Section 7 we present the benefit of the synergistic use of physical and digital evidences to facilitate trustworthy operations of cyber systems.

We believe that only if we tackle these challenges right, we can turn the science fiction of UbiComp into science fact.

Particularly, we choose to address the areas above because they represent promising research directions e cover different aspects of UbiComp security and privacy.

**Software protection**

Modern UbiComp systems are rarely built from scratch. Components developed by different organizations, with different programming models and tools, and under different assumptions are integrated to offer complex capabilities. In this section, we analyze the software ecosystem that emerges from such a world. Figure [2](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig2) provides a high-level representation of this ecosystem. In the rest of this section, we shall focus specially on three aspects of this environment, which pose security challenges to developers: the security shortcomings of C and C++, the dominant programming languages among cyber-physical implementations; the interactions between these languages and other programming languages, and the consequences of these interactions on the distributed nature of UbiComp applications. We start by diving deeper into the idiosyncrasies of C and C++.



**Type safety**

A great deal of the software used in UbiComp systems is implemented in C or in C++. This fact is natural, given the unparalleled efficiency of these two programming languages. However, if, on the one hand, C and C++ yield efficient executables, on the other hand, their weak type system gives origin to a plethora of software vulnerabilities. In programming language’s argot, we say that a type system is weak when it does not support two key properties: progress and preservation [[14](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR14" \o "Pierce BC. Types and programming languages, 1st edition. Cambridge: The MIT Press; 2002.)]. The formal definitions of these properties are immaterial for the discussion that follows. It suffices to know that, as a consequence of weak typing, neither C, nor C++, ensure, for instance, bounded memory accesses. Therefore, programs written in these languages can access invalid memory positions. As an illustration of the dangers incurred by this possibility, it suffices to know that out-of-bounds access are the principle behind buffer overflow exploits.

The software security community has been developing different techniques to deal with the intrinsic vulnerabilities of C/C++/assembly software. Such techniques can be fully static, fully dynamic or a hybrid of both approaches. Static protection mechanisms are implemented at the compiler level; dynamic mechanisms are implemented at the runtime level. In the rest of this section, we list the most well-known elements in each category.

Static analyses provide a conservative estimate of the program behavior, without requiring the execution of such a program. This broad family of techniques includes, for instance, abstract interpretation [[15](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR15" \o "Cousot P, Cousot R. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: POPL. New York: ACM: 1977. p. 238–52.)], model checking [[16](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR16" \o "McMillan KL. Symbolic model checking. Norwell: Kluwer Academic Publishers; 1993.)] and guided proofs [[17](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR17" \o "Leroy X. Formal verification of a realistic compiler. Commun ACM. 2009; 52(7):107–15.)]. The main advantage of static analyses is the low runtime overhead, and its soundness: inferred properties are guaranteed to always hold true. However, static analyses have also disadvantages. In particular, most of the interesting properties of programs lay on undecidable land [[18](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR18" \o "Rice HG. Classes of recursively enumerable sets and their decision problems. Trans Amer Math Soc. 1953; 74(1):358–66.)]. Furthermore, the verification of many formal properties, even though a decidable problem, incur a prohibitive computational cost [[19](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR19" \o "Wilson RP, Lam MS. Efficient context-sensitive pointer analysis for c programs. In: PLDI. New York: ACM: 1995. p. 1–12.)].

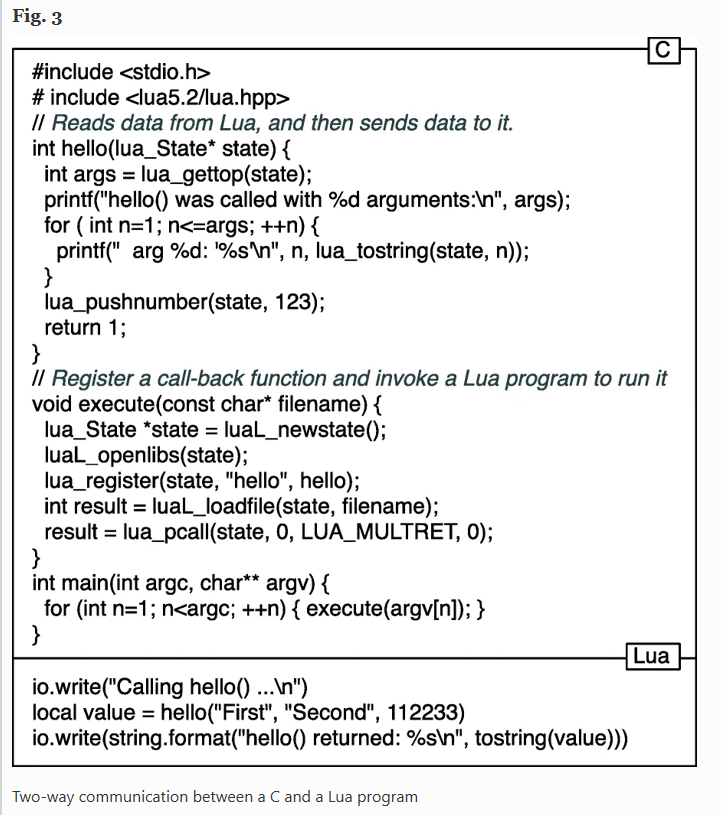
Dynamic analyses come in several flavors: testing (KLEE [[20](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR20" \o "Cadar C, Dunbar D, Engler D. KLEE: Unassisted and automatic generation of high-coverage tests for complex systems programs. In: OSDI. Berkeley: USENIX: 2008. p. 209–24.)]), profiling (Aprof [[21](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR21" \o "Coppa E, Demetrescu C, Finocchi I. Input-sensitive profiling. In: PLDI. New York: ACM: 2012. p. 89–98.)], Gprof [[22](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR22" \o "Graham SL, Kessler PB, McKusick MK. gprof: a call graph execution profiler (with retrospective). In: Best of PLDI. New York: ACM: 1982. p. 49–57.)]), symbolic execution (DART [[23](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR23" \o "Godefroid P, Klarlund N, Sen K. Dart: directed automated random testing. In: PLDI. New York: ACM: 2005. p. 213–23.)]), emulation (Valgrind [[24](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR24" \o "Nethercote N, Seward J. Valgrind: a framework for heavyweight dynamic binary instrumentation. In: PLDI. New York: ACM: 2007. p. 89–100.)]), and binary instrumentation (Pin [[25](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR25" \o "Luk C-K, Cohn R, Muth R, Patil H, Klauser A, Lowney G, Wallace S, Reddi VJ, Hazelwood K. Pin: Building customized program analysis tools with dynamic instrumentation. In: PLDI. New York: ACM: 2005. p. 190–200.)]). The virtues and limitations of dynamic analyses are exactly the opposite of those found in static techniques. Dynamic analyses usually do not raise false alarms: bugs are described by examples, which normally lead to consistent reproduction [[26](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR26" \o "Rimsa AA, D’Amorim M, Pereira FMQ. Tainted flow analysis on e-SSA-form programs. In: CC. Berlin: Springer: 2011. p. 124–43.)]. However, they are not required to always find security vulnerabilities in software. Furthermore, the runtime overhead of dynamic analyses still makes it prohibitive to deploy them into production software [[27](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR27" \o "Serebryany K, Bruening D, Potapenko A, Vyukov D. Addresssanitizer: a fast address sanity checker. In: ATC. Berkeley: USENIX: 2012. p. 28.)].

As a middle point, several research groups have proposed ways to combine static and dynamic analyses, producing different kinds of hybrid approaches to secure low-level code. This combination might yield security guarantees that are strictly more powerful than what could be obtained by either the static or the dynamic approaches, when used separately [[28](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR28" \o "Russo A, Sabelfeld A. Dynamic vs. static flow-sensitive security analysis. In: CSF. Washington: IEEE: 2010. p. 186–99.)]. Nevertheless, negative results still hold: if an attacker can take control of the program, usually he or she can circumvent state-of-the-art hybrid protection mechanisms, such as control flow integrity [[29](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR29" \o "Carlini N, Barresi A, Payer M, Wagner D, Gross TR. Control-flow bending: On the effectiveness of control-flow integrity. In: SEC. Berkeley: USENIX: 2015. p. 161–76.)]. This fact is, ultimately, a consequence of the weak type system adopted by languages normally seen in the implementation of UbiComp systems. Therefore, the design and deployment of techniques that can guard such programming languages, without compromising their efficiency to the point where they will no longer be adequate to UbiComp development, remains an open problem.

In spite of the difficulties of bringing formal methods to play a larger role in the design and implementation of programming languages, much has already been accomplished in this field. Testimony to this statement is the fact that today researchers are able to ensure the safety of entire operating system kernels, as demonstrated by Gerwin et al. [[30](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR30" \o "Klein G, Elphinstone K, Heiser G, Andronick J, Cock D, Derrin P, Elkaduwe D, Engelhardt K, Kolanski R, Norrish M, Sewell T, Tuch H, Winwood S. sel4: Formal verification of an os kernel. In: SOSP. New York: ACM: 2009. p. 207–20.)], and to ensure that compilers meet the semantics of the languages that they process [[31](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR31" \o "Jourdan J-H, Laporte V, Blazy S, Leroy X, Pichardie D. A formally-verified c static analyzer. In: POPL. New York: ACM: 2015. p. 247–59.)]. Nevertheless, it is reasonable to think that certain safety measures might come at the cost of performance and therefore we foresee that much of the effort of the research community in the coming years will be dedicated to making formal methods not only more powerful and expressive, but also more efficient to be used in practice.

**Polyglot programming**

Polyglot programming is the art and discipline of writing source code that involves two or more programming languages. It is common among implementations of cyber-physical systems. As an example, Ginga, the Brazilian protocol for digital TV, is mostly implemented in Lua and C [[32](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR32" \o "Soares LFG, Rodrigues RF, Moreno MF. Ginga-NCL: the declarative environment of the brazilian digital tv system. J Braz Comp Soc. 2007; 12(4):1–10.)]. Figure [3](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig3) shows an example of communication between a C and a Lua program. Other examples of interactions between programming languages include bindings between C and Python [[33](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR33" \o "Maas AJ, Nazaré H, Liblit B. Array length inference for c library bindings. In: ASE. New York: ACM: 2016. p. 461–71.)], C and Elixir [[34](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR34" \o "Fedrecheski G, Costa LCP, Zuffo MK. ISCE. Washington: IEEE: 2016.)] and the Java Native Interface [[35](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR35" \o "Rellermeyer JS, Duller M, Gilmer K, Maragkos D, Papageorgiou D, Alonso G. The software fabric for the internet of things. In: IOT. Berlin, Heidelberg: Springer-Verlag: 2008. p. 87–104.)]. Polyglot programming complicates the protection of systems. Difficulties arise due to a lack of multi-language tools and due to unchecked memory bindings between C/C++ and other languages.



An obstacle to the validation of polyglot software is the lack of tools that analyze source code written in different programming languages, under a unified framework. Returning to Fig. [3](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig3), we have a system formed by two programs, written in different programming languages. Any tool that analyzes this system as a whole must be able to parse these two distinct syntaxes and infer the connection points between them. Work has been performed towards this end, but solutions are still very preliminary. As an example, Maas et al. [[33](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR33" \o "Maas AJ, Nazaré H, Liblit B. Array length inference for c library bindings. In: ASE. New York: ACM: 2016. p. 461–71.)] have implemented automatic ways to check if C arrays are correctly read by Python programs. As another example, Furr and Foster [[36](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR36" \o "Furr M, Foster JS. Checking type safety of foreign function calls. ACM Trans Program Lang Syst. 2008; 30(4):18:1–18:63.)] have described techniques to ensure type-safety of OCaml-to-C and Java-to-C bindings.

A promising direction to analyze polyglot systems is based on the idea of compilation of source code partially available. This feat consists in the reconstruction of the missing syntax and the missing declarations necessary to produce a minimal version of the original program that can be analyzed by typical tools. The analysis of code partially available makes it possible to test parts of a polyglot program in separate, in a way to produce a cohesive view of the entire system. This technique has been demonstrated to yield analyzable Java source code [[37](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR37" \o "Dagenais B, Hendren L. OOPSLA. New York: ACM: 2008. p. 313–28.)], and compilable C code [[38](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR38" \o "Melo LTC, Ribeiro RG, de Araújo MR, Pereira FMQ. Inference of static semantics for incomplete c programs. Proc ACM Program Lang. 2017; 2(POPL):29:1–29:28.)]. Notice that this type of reconstruction is not restricted to high-level programming languages. Testimony of this fact is the notion of micro execution, introduced by Patrice Godefroid [[39](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR39" \o "Godefroid P. Micro execution. In: ICSE. New York: ACM: 2014. p. 539–49.)]. Godefroid’s tool allows the testing of x86 binaries, even when object files are missing. Nevertheless, in spite of these developments, the reconstruction is still restricted to the static semantics of programs. The synthesis of behavior is a thriving discipline in computer science [[40](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR40" \o "Manna Z, Waldinger RJ. Toward automatic program synthesis. Commun ACM. 1971; 14(3):151–65.)], but still far away from enabling the certification of polyglot systems.

**Distributed programming**

Ubiquitous computing systems tend to be distributed. It is even difficult to conceive any use for an application in this world that does not interact with other programs. And it is common knowledge that distributed programming opens up several doors to malicious users. Therefore, to make cyber-physical technology safer, security tools must be aware of the distributed nature of such systems. Yet, two main challenges stand in front of this requirement: the difficulty to build a holistic view of the distributed application, and the lack of semantic information bound to messages exchanged between processes that communicate through a network.

To be accurate, the analysis of a distributed system needs to account for the interactions between the several program parts that constitute this system [[41](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR41" \o "López HA, Marques ERB, Martins F, Ng N, Santos C, Vasconcelos VT, Yoshida N. Protocol-based verification of message-passing parallel programs. In: OOPSLA. New York: ACM: 2015. p. 280–98.)]. Discovering such interactions is difficult, even if we restrict ourselves to code written in a single programming language. Difficulties stem from a lack of semantic information associated with operations that send and receive messages. In other words, such operations are defined as part of a library, not as part of the programming language itself. Notwithstanding this fact, there are several techniques that infer communication channels between different pieces of source code. As examples, we have the algorithms of Greg Bronevetsky [[42](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR42" \o "Bronevetsky G. Communication-sensitive static dataflow for parallel message passing applications. In: CGO. Washington: IEEE: 2009. p. 1–12.)], and Teixeira et al. [[43](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR43" \o "Teixeira FA, Machado GV, Pereira FMQ, Wong HC, Nogueira JMS, Oliveira LB. Siot: Securing the internet of things through distributed system analysis. In: IPSN. New York: ACM: 2015. p. 310–21.)], which build a distributed view of a program’s control flow graph (CFG). Classic static analyses work without further modification on this distributed CFG. However, the distributed CFG is still a conservative approximation of the program behavior. Thus, it forces already imprecise static analyses to deal with communication channels that might never exist during the execution of the program. The rising popularization of actor-based libraries, like those available in languages such as Elixir [[34](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR34" \o "Fedrecheski G, Costa LCP, Zuffo MK. ISCE. Washington: IEEE: 2016.)] and Scala [[44](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR44" \o "Lhoták O, Hendren L. Context-sensitive points-to analysis: Is it worth it? In: CC. Berlin, Heidelberg: Springer: 2006. p. 47–64.)] is likely to mitigate the channel-inference problem. In the actor model channels are explicit in the messages exchanged between the different processing elements that constitute a distributed system. Nevertheless, if such model will be widely adopted by the IoT community is still a fact to be seen.

Tools that perform automatic analyses in programs rely on static information to produce more precise results. In this sense, types are core for the understanding of software. For instance, in Java and other object-oriented languages, the type of objects determines how information flows along the program code. However, despite this importance, messages exchanged in the vast majority of distributed systems are not typed. Reason for this is the fact that such messages, at least in C, C++ and assembly software, are arrays of bytes. There have been two major efforts to mitigate this problem: the addition of messages as first class values to programming languages, and the implementation of points-to analyses able to deal with pointer arithmetics in languages that lack such feature. Concerning the first front, several programming languages, such as Scala, Erlang and Elixir, incorporate messages as basic constructs, providing developers with very expressive ways to implement the actor model [[45](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR45" \o "Agha G. An overview of actor languages. In: OOPWORK. New York: ACM: 1986. p. 58–67.)] – a core foundation of distributed programming. Even though the construction of programming abstractions around the actor model is not a new idea [[45](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR45" \o "Agha G. An overview of actor languages. In: OOPWORK. New York: ACM: 1986. p. 58–67.)], their raising popularity seems to be a phenomenon of the 2000’s, boosted by increasingly more expressive abstractions [[46](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR46" \o "Haller P, Odersky M. Actors that unify threads and events. In: Proceedings of the 9th International Conference on Coordination Models and Languages. COORDINATION’07. Berlin, Heidelberg: Springer-Verlag: 2007. p. 171–90.)] and increasingly more efficient implementations [[47](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR47" \o "Imam SM, Sarkar V. Integrating task parallelism with actors. In: OOPSLA. New York: ACM: 2012. p. 753–72.)]. In the second front, researchers have devised analyses that infer the contents [[48](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR48" \o "Cousot P, Cousot R, Logozzo F. A parametric segmentation functor for fully automatic and scalable array content analysis. In: POPL. New York: ACM: 2011. p. 105–18.)] and the size of arrays [[49](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR49" \o "Nazaré H, Maffra I, Santos W, Barbosa L, Gonnord L, Pereira FMQ. Validation of memory accesses through symbolic analyses. In: OOPSLA. New York: ACM: 2014.)] in weakly-typed programming languages. More importantly, recent years have seen a new flurry of algorithms designed to analyze C/C++ style pointer arithmetics [[50](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR50" \o "Paisante V, Maalej M, Barbosa L, Gonnord L, Pereira FMQ. Symbolic range analysis of pointers. In: CGO. New York: ACM: 2016. p. 171–81.)–[53](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR53" \o "Sui Y, Fan X, Zhou H, Xue J. Loop-oriented pointer analysis for automatic simd vectorization. ACM Trans Embed Comput Syst. 2018; 17(2):56:1–56:31.)]. The wide adoption of higher-level programming languages coupled with the construction of new tools to analyze lower-level languages is exciting. This trend seems to indicate that the programming languages community is dedicating each time more attention to the task of implementing safer distributed software. Therefore, even though the design of tools able to analyze the very fabric of UbiComp still poses several challenges to researchers, we can look to the future with optimism.

**Long-term security**

Various UbiComp systems are designed to withstand a lifespan of many years, even decades [[54](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR54" \o "Poovendran R. Cyber-physical systems: Close encounters between two parallel worlds [point of view]. Proc IEEE. 2010; 98(8):1363–6.), [55](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR55" \o "Conti JP. The internet of things. Commun Eng. 2006; 4(6):20–5.)]. Systems in the context of critical infrastructure, for example, often require an enormous financial investment to be designed and deployed in the field [[56](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR56" \o "Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. 2001; 21(6):11–25.)], and therefore would offer a better return on investment if they remain in use for a longer period of time. The automotive area is a field of particular interest. Vehicles are expected to be reliable for decades [[57](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR57" \o "US Bureau of Transportation Statistics BTS. Average age of automobiles and trucks in operation in the united states. 2017. Accessed 14 Sept 2017.)], and renewing vehicle fleets or updating features (recalls) increase costs for their owners. Note that modern vehicles are part of the UbiComp ecosystem as they are equipped with embedded devices with Internet connectivity. In the future, it is expected that vehicles will depend even more on data collected and shared across other vehicles/infrastructure through wireless technologies [[58](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR58" \o "U.S. Department of Transportation. IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments WAVE. 2013.)] in order to enable enriched driving experiences such as autonomous driving [[59](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR59" \o "Maurer M, Gerdes JC, Lenz B, Winner H. Autonomous driving: technical, legal and social aspects.Berlin: Springer; 2016.)].

It is also worth mentioning that systems designed to endure a lifespan of several years or decades might suffer from lack of future maintenance. The competition among players able to innovate is very aggressive leading to a high rate of companies going out of business within a few years [[60](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR60" \o )]. A world inundate by devices without proper maintenance will offer serious future challenges [[61](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR61" \o "Jacobsson A, Boldt M, Carlsson B. A risk analysis of a smart home automation system. Futur Gener Comput Syst. 2016; 56(Supplement C):719–33.)].

From the few aforementioned examples, it is already evident that there is an increasing need for UbiComp systems to be reliable for a longer period of time and, whenever possible, requiring as few updates as possible. These requirements have a direct impact on the security features of such systems: comparatively speaking, they would offer fewer opportunities for patching eventual security breaches than conventional systems. This is a critical situation given the intense and dynamic progresses on devising and exploiting new security breaches. Therefore, it is of utmost importance to understand what the scientific challenges are to ensure long-term security from the early stage of the design of an UbiComp system, instead of resorting to palliative measures a posteriori.

**Cryptography as the core component**

Ensuring long-term security is a quite challenging task for any system, not only for UbiComp systems. At a minimum, it requires that every single security component is future-proof by itself and also when connected to other components. To simplify this excessively large attack surface and still be able to provide helpful recommendations, we will focus our attention on the main ingredient of most security mechanisms, as highlighted in Section [4](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec10), i.e. Cryptography.

There are numerous types of cryptographic techniques. The most traditional ones rely on the hardness of computational problems such as integer factorization [[62](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR62" \o "Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978; 21(2):120–6.)] and discrete logarithm problems [[63](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR63" \o "Miller VS. Use of elliptic curves in cryptography. In: CRYPTO, volume 218 of Lecture Notes in Computer Science. Berlin: Springer: 1985. p. 417–26.), [64](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR64" \o "Koblitz N. Elliptic curve cryptosystems. Math Comput. 1987; 48(177):203–9.)]. These problems are believed to be intractable by current cryptanalysis techniques and the available technological resources. Because of that, cryptographers were able to build secure instantiation of cryptosystems based on such computational problems. For various reasons (to be discussed in the following sections), however, the future-proof condition of such schemes is at stake.

**Advancements in classical cryptanalysis**

The first threat for the future-proof condition of any cryptosystem refers to potential advancements on cryptanalysis, i.e., on techniques aiming at solving the underlying security problem in a more efficient way (with less processing time, memory, etc.) than originally predicted. Widely-deployed schemes have a long track of academic and industrial scrutiny and therefore one would expect little or no progress on the cryptanalysis techniques targeting such schemes. Yet, the literature has recently shown some interesting and unexpected results that may suggest the opposite.

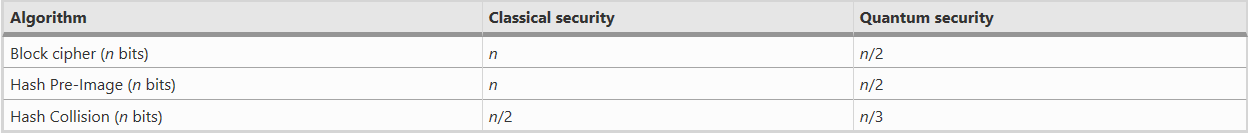
In [[65](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR65" \o "Barbulescu R, Gaudry P, Joux A, Thomé E. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: EUROCRYPT 2014. Berlin: Springer: 2014. p. 1–16.)], for example, Barbulescu et al. introduced a new quasi-polynomial algorithm to solve the discrete logarithm problem in finite fields of small characteristics. The discrete logarithm problem is the underlying security problem of the Diffie-Hellman Key Exchange [[66](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR66" \o "Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theor. 2006; 22(6):644–54.)], the Digital Signature Algorithm [[67](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR67" \o "Barker E. Federal Information Processing Standards Publication (FIPS PUB) 186-4 Digital Signature Standard (DSS). 2013.)] and their elliptic curve variants (ECDH [[68](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR68" \o "Barker E, Johnson D, Smid M. Special publication 800-56A recommendation for pair-wise key establishment schemes using discrete logarithm cryptography. 2006.)] and ECDSA [[67](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR67" \o "Barker E. Federal Information Processing Standards Publication (FIPS PUB) 186-4 Digital Signature Standard (DSS). 2013.)], respectively), just to mention a few widely-deployed cryptosystems. This cryptanalytic result is restricted to finite fields of small characteristics, something that represents an important limitation to attack real-world implementations of the aforementioned schemes. However, any sub-exponential algorithm that solves a longstanding problem should be seen as a relevant indication that the cryptanalysis literature might still be subject to eventual breakthroughs.

This situation should be considered by architects designing UbiComp systems that have long-term security as a requirement. Implementations that support various (i.e. higher than usual) security levels are preferred when compared to fixed, single key size support. The same approach used for keys should be used to other quantities in the scheme that somehow impact on its overall security. In this way, UbiComp systems would be able to consciously accommodate future cryptanalytic advancements or, at the very least, reduce the costs for security upgrades.

**Future disruption due to quantum attacks**

Quantum computers are expected to offer dramatic speedups to solve certain computational problems, as foreseen by Daniel R. Simon in his seminal paper on quantum algorithms [[69](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR69" \o "Simon DR. On the power of quantum computation. In: Symposium on Foundations of Computer Science (SFCS 94). Washington: IEEE Computer Society: 1994. p. 116–23.)]. Some of these speedups may enable significant advancements to technologies currently limited by its algorithmic inefficiency [[70](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR70" \o "Knill E. Physics: quantum computing. Nature. 2010; 463(7280):441–3.)]. On the other hand, to our misfortune, some of the affected computational problems are the ones currently being used to secure widely-deployed cryptosystems.

As an example, Lov K. Grover introduced a quantum algorithm [[71](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR71" \o "Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of ACM STOC 1996. New York: ACM: 1996. p. 212–19.)] able to find an element in the domain of a function (of size N) which leads, with high probability, to a desired output in only O(N−−√)O(N) steps. This algorithm can be used to speed up the cryptanalysis of symmetric cryptography. Block ciphers of n bits keys, for example, would offer only n/2 bits of security against a quantum adversary. Hash functions would be affected in ways that depend on the expected security property. In more details, hash functions of n bits digests would offer only n/3 bits of security against collision attacks and n/2 bits of security against pre-image attacks. Table [1](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Tab1) summarizes this assessment. In this context, AES-128 and SHA-256 (collision-resistance) would not meet the minimum acceptable security level of 128-bits (of quantum security). Note that both block ciphers and hash function constructions will still remain secure if longer keys and digest sizes are employed. However, this would lead to important performance challenges. AES-256, for example, is about 40% less efficient than AES-128 (due to the 14 rounds, instead of 10).



Even more critical than the scenario for symmetric cryptography, quantum computers will offer an exponential speedup to attack most of the widely-deployed public-key cryptosystems. This is due to Peter Shor’s algorithm [[72](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR72" \o "Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput. 1997; 26(5):1484–509.)] which can efficiently factor large integers and compute the discrete logarithm of an element in large groups in polynomial time. The impact of this work will be devastating to RSA and ECC-based schemes as increasing the key sizes would not suffice: they will need to be completely replaced.

In the field of quantum resistant public-key cryptosystems, i.e. alternative public key schemes that can withstand quantum attacks, several challenges need to be addressed. The first one refers to establishing a consensus in both academia and industry on how to defeat quantum attacks. In particular, there are two main techniques considered as capable to withstand quantum attacks, namely: post-quantum cryptography (PQC) and quantum cryptography (QC). The former is based on different computational problems believed to be so hard that not even quantum computers would be able to tackle them. One important benefit of PQC schemes is that they can be implemented and deployed in the computers currently available [[73](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR73" \o "McEliece RJ. A public-key cryptosystem based on algebraic coding theory. Deep Space Netw. 1978; 44:114–6.)–[77](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR77" \o )]. The latter (QC) depends on the existence and deployment of a quantum infrastructure, and is restricted to key-exchange purposes [[78](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR78" \o "Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE ICCSSP’84. New York: IEEE Press: 1984. p. 175–9.)]. The limited capabilities and the very high costs for deploying quantum infrastructure should eventually lead to a consensus towards the post-quantum cryptography trend.

There are several PQC schemes available in the literature. Hash-Based Signatures (HBS), for example, are the most accredited solutions for digital signatures. The most modern constructions [[76](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR76" \o "Buchmann J, Dahmen E, Hülsing A. Xmss - a practical forward secure signature scheme based on minimal security assumptions In: Yang B-Y, editor. PQCrypto. Berlin: Springer: 2011. p. 117–29.), [77](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR77" \o )] represent improvements of the Merkle signature scheme [[74](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR74" \o "Merkle RC. Secrecy, authentication and public key systems / A certified digital signature. PhD thesis, Stanford. 1979.)]. One important benefit of HBS is that their security relies solely on certain well-known properties of hash functions (thus they are secure against quantum attacks, assuming appropriate digest sizes are used). Regarding other security features, such as key exchange and asymmetric encryption, the academic and industry communities have not reached a consensus yet, although both code-based and lattice-based cryptography literatures have already presented promising schemes [[79](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR79" \o )–[85](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR85" \o "Barreto PSLM, Gueron S, Gueneysu T, Misoczki R, Persichetti E, Sendrier N, Tillich J-P. Cake: Code-based algorithm for key encapsulation. In: IMA International Conference on Cryptography and Coding. Berlin: Springer: 2017. p. 207–26.)]. Isogeny-based cryptography [[86](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR86" \o "Jao D, De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: International Workshop on Post-Quantum Cryptography. Berlin: Springer: 2011. p. 19–34.)] is a much more recent approach that enjoys certain practical benefits (such as fairly small public key sizes [[87](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR87" \o "Costello C, Jao D, Longa P, Naehrig M, Renes J, Urbanik D. Efficient compression of sidh public keys. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer: 2017. p. 679–706.), [88](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR88" \o )]) although it has just started to benefit from a more comprehensive understanding of its cryptanalysis properties [[89](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR89" \o "Galbraith SD, Petit C, Shani B, Ti YB. On the security of supersingular isogeny cryptosystems. In: International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer: 2016. p. 63–91.)]. Regarding standardization efforts, NIST has recently started a Standardization Process on Post-Quantum Cryptography schemes [[90](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR90" \o )] which should take at least a few more years to be concluded. The current absence of standards represents an important challenge. In particular, future interoperability problems might arise.

Finally, another challenge in the context of post-quantum public-key cryptosystems refers to potentially new implementation requirements or constraints. As mentioned before, hash-based signatures are very promising post-quantum candidates (given efficiency and security related to hash functions) but also lead to a new set of implementation challenges, such as the task of keeping the scheme state secure. In more details, most HBS schemes have private-keys (their state) that evolve along the time. If rigid state management policies are not in place, a signer can re-utilize the same private-key twice, something that would void the security guarantees offered by the scheme. Recently, initial works to address these new implementation challenges have appeared in the literature [[91](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR91" \o "McGrew D, Kampanakis P, Fluhrer S, Gazdag S-L, Butin D, Buchmann J. State management for hash-based signatures. In: International Conference on Research in Security Standardization. Springer: 2016. p. 244–60.)]. A recently introduced HBS construction [[92](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR92" \o "Bernstein DJ, Hopwood D, Hülsing A, Lange T, Niederhagen R, Papachristodoulou L, Schneider M, Schwabe P, Wilcox-O’Hearn Z. SPHINCS: Practical Stateless Hash-Based Signatures. Berlin, Heidelberg: Springer Berlin Heidelberg; 2015. p. 368–97.)] showed how to get rid of the state management issue at the price of much larger signatures. These examples indicate potentially new implementation challenges for PQC schemes that must be addressed by UbiComp systems architects.

**Cryptographic engineering**

UbiComp systems involve building blocks of very different natures: hardware components such as sensors and actuators, embedded software implementing communication protocols and interface with cloud providers, and ultimately operational procedures and other human factors. As a result, pervasive systems have a large attack surface that must be protected using a combination of techniques.

Cryptography is a fundamental part of any modern computing system, but unlikely to be the weakest component in its attack surface. Networking protocols, input parsing routines and even interface code with cryptographic mechanisms are components much more likely to be vulnerable to exploitation. However, a successful attack on cryptographic security properties is usually disastrous due to the risk concentrated in cryptographic primitives. For example, violations of confidentiality may cause massive data breaches involving sensitive information. Adversarial interference on communication integrity may allow command injection attacks that deviate from the specified behavior. Availability is crucial to keep the system accessible by legitimate users and to guarantee continuous service provisioning, thus cryptographic mechanisms must also be lightweight to minimize potential for abuse by attackers.

Physical access by adversaries to portions of the attack surface is a particularly challenging aspect of deploying cryptography in UbiComp systems. By assumption, adversaries can recover long-term secrets and credentials that provide some control over a (hopefully small) portion of the system. Below we will explore some of the main challenges in deploying cryptographic mechanisms for pervasive systems, including how to manage keys and realize efficient and secure implementation of cryptography.

**Key management**

UbiComp systems are by definition heterogeneous platforms, connecting devices of massively different computation and storage power. Designing a cryptographic architecture for any heterogeneous system requires assigning clearly defined roles and corresponding security properties for the tasks under responsibility of each entity in the system. Resource-constrained devices should receive less computationally intensive tasks, and their lack of tamper-resistance protections indicate that long-term secrets should not reside in these devices. More critical tasks involving expensive public-key cryptography should be delegated to more powerful nodes. A careful trade-off between security properties, functionality and cryptographic primitives must then be addressed per device or class of devices [[93](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR93" \o "Barker E, Barker W, Burr W, Polk W, Smid M. Recommendation for key management part 1: General (revision 3). NIST Spec Publ. 2012; 800(57):1–147.)], following a set of guidelines for pervasive systems:

* Functionality: key management protocols must manage lifetime of cryptographic keys and ensure accessibility to the currently authorized users, but handling key management and authorization separately may increase complexity and vulnerabilities. A promising way of combining the two services into a cryptographically-enforced access control framework is attribute-based encryption [[94](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR94" \o "Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Public Key Cryptography. LNCS, 6571 vol.Berlin: Springer: 2011. p. 53–70.), [95](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR95" \o "Liu Z, Wong DS. Practical attribute-based encryption: Traitor tracing, revocation and large universe. Comput J. 2016; 59(7):983–1004.)], where keys have sets of capabilities and attributes that can be authorized and revoked on demand.
* Communication: components should minimize the amount of communication, at risk of being unable to operate if communication is disrupted. Non-interactive approaches for key distribution [[96](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR96" \o "Oliveira LB, Aranha DF, Gouvêa CPL, Scott M, Câmara DF, López J, Dahab R. Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Comput Commun. 2011; 34(3):485–93.)] are recommended here, but advanced protocols based on bilinear pairings should be avoided due to recent advances on solving the discrete log problem (in the so called medium prime case [[97](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR97" \o "Kim T, Barbulescu R. Extended tower number field sieve: A new complexity for the medium prime case. In: CRYPTO (1). LNCS, 9814 vol.Berlin: Springer: 2016. p. 543–71.)]). These advances forcedly increase the parameter sizes, reduce performance/scalability and may be improved further, favoring more traditional forms of asymmetric cryptography.
* Efficiency: protocols should be lightweight and easy to implement, mandating that traditional public key infrastructures (PKIs) and expensive certificate handling operations are restricted to the more powerful and connected nodes in the architecture. Alternative models supporting implicit certification include identity-based [[98](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR98" \o "Boneh D, Franklin MK. Identity-based encryption from the weil pairing. SIAM J Comput. 2003; 32(3):586–615.)] (IBC) and certificate-less cryptography [[99](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR99" \o "Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: ASIACRYPT. LNCS, 2894 vol.Berlin: Springer: 2003. p. 452–73.)] (CLPKC), the former implying inherent key escrow. The difficulties with key revocation still impose obstacles for their wide adoption, despite progress [[100](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR100" \o "Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation. IACR Cryptol ePrint Arch. 2012; 2012:52.)]. A lightweight pairing and escrow-less authenticated key agreement based on an efficient key exchange protocol and implicit certificates combines the advantages of the two approaches, providing high performance while saving bandwidth [[101](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR101" \o "Simplício Jr. MA, Silva MVM, Alves RCA, Shibata TKC. Lightweight and escrow-less authenticated key agreement for the internet of things. Comput Commun. 2017; 98:43–51.)].
* Interoperability: pervasive systems are composed of components originating from different manufacturers. Supporting a cross-domain authentication and authorization framework is crucial for interoperability [[102](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR102" \o "Neto ALM, Souza ALF, Cunha ÍS, Nogueira M, Nunes IO, Cotta L, Gentille N, Loureiro AAF, Aranha DF, Patil HK, Oliveira LB. Aot: Authentication and access control for the entire iot device life-cycle. In: SenSys. New York: ACM: 2016. p. 1–15.)].

Cryptographic primitives involved in joint functionality must then be compatible with all endpoints and respect the constraints of the less powerful devices.

**Lightweight cryptography**

The emergence of huge collections of interconnected devices in UbiComp motivate the development of novel cryptographic primitives, under the moniker lightweight cryptography. The term lightweight does not imply weaker cryptography, but application-tailored cryptography that is especially designed to be efficient in terms of resource consumption such as processor cycles, energy and memory footprint [[103](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR103" \o "Mouha N. The design space of lightweight cryptography. IACR Cryptol ePrint Arch. 2015; 2015:303.)]. Lightweight designs aim to target common security requirements for cryptography but may adopt less conservative choices or more recent building blocks.

As a first example, many new block ciphers were proposed as lightweight alternatives to the Advanced Encryption Standard (AES) [[104](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR104" \o "Daemen J, Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Berlin: Springer; 2002.)]. Important constructions are LS-Designs [[105](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR105" \o "Grosso V, Leurent G, Standaert F-X, Varici K. Ls-designs: Bitslice encryption for efficient masked software implementations. In: FSE. LNCS, 8540 vol.Berlin: Springer: 2014. p. 18–37.)], modern ARX and Feistel networks [[106](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR106" \o "Dinu D, Perrin L, Udovenko A, Velichkov V, Großschädl J, Biryukov A. Design strategies for ARX with provable bounds: Sparx and LAX. In: ASIACRYPT (1). LNCS, 10031 vol.Berlin: Springer: 2016. p. 484–513.)], and substitution-permutation networks [[107](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR107" \o "Albrecht MR, Driessen B, Kavun EB, Leander G, Paar C, Yalçin T. Block ciphers - focus on the linear layer (feat. PRIDE). In: CRYPTO (1). LNCS, 8616 vol.Berlin: Springer: 2014. p. 57–76.), [108](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR108" \o "Beierle C, Jean J, Kölbl S, Leander G, Moradi A, Peyrin T, Sasaki Y, Sasdrich P, Sim SM. The SKINNY family of block ciphers and its low-latency variant MANTIS. In: CRYPTO (2). LNCS, 9815 vol.Berlin: Springer: 2016. p. 123–53.)]. A notable candidate is the PRESENT block cipher, with a 10-year maturity of resisting cryptanalytic attempts [[109](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR109" \o "Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJB, Seurin Y, Vikkelsoe C. PRESENT: an ultra-lightweight block cipher. In: CHES. LNCS, 4727 vol.Berlin: Springer: 2007. p. 450–66.)], and whose performance recently became competitive in software [[110](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR110" \o "Reis TBS, Aranha DF, López J. PRESENT runs fast - efficient and secure implementation in software. In: CHES, volume 10529 of Lecture Notes in Computer Science. Berlin: Springer: 2017. p. 644–64.)].

In the case of hash functions, a design may even trade-off advanced security properties (such as collision resistance) for simplicity in some scenarios. A clear case is the construction of short Message Authentication Codes (MAC) from non-collision resistant hash functions, such as in SipHash [[111](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR111" \o "Aumasson J-P, Bernstein DJ. Siphash: A fast short-input PRF. In: INDOCRYPT. LNCS, 7668 vol.Berlin: Springer: 2012. p. 489–508.)], or digital signatures from short-input hash functions [[112](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR112" \o "Kölbl S, Lauridsen MM, Mendel F, Rechberger C. Haraka v2 - efficient short-input hashing for post-quantum applications. IACR Trans Symmetric Cryptol. 2016; 2016(2):1–29.)]. In conventional applications, BLAKE2 [[113](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR113" \o "Aumasson J-P, Neves S, Wilcox-O’Hearn Z, Winnerlein C. BLAKE2: simpler, smaller, fast as MD5. In: ACNS. LNCS, 7954 vol.Berlin: Springer: 2013. p. 119–35.)] is a stronger drop-in replacement to recently cryptanalyzed standards [[114](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR114" \o "Stevens M, Karpman P, Peyrin T. Freestart collision for full SHA-1. In: EUROCRYPT (1). LNCS, 9665 vol.Berlin: Springer: 2016. p. 459–83.)] and faster in software than the recently published SHA-3 standard [[115](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR115" \o "NIST Computer Security Division. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. FIPS Publication 202, National Institute of Standards and Technology, U.S. Department of Commerce, May 2014.)].

Another trend is to provide confidentiality and authentication in a single step, through Authenticated Encryption with Associated Data (AEAD). This can be implemented with a block cipher operation mode (like GCM [[116](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR116" \o "McGrew DA, Viega J. The security and performance of the galois/counter mode (GCM) of operation. In: INDOCRYPT. LNCS, 3348 vol.Berlin: Springer: 2004. p. 343–55.)]) or a dedicated design. The CAESAR competition selected new AEAD algorithms for standardization across multiple use cases, such as lightweight and high-performance applications and a defense-in-depth setting. NIST has followed through and started its own standardization process for lightweight AEAD algorithms and hash functions.

In terms of public-key cryptography, Elliptic Curve Cryptography (ECC) [[63](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR63" \o "Miller VS. Use of elliptic curves in cryptography. In: CRYPTO, volume 218 of Lecture Notes in Computer Science. Berlin: Springer: 1985. p. 417–26.), [117](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR117" \o "Koblitz N. A family of jacobians suitable for discrete log cryptosystems. In: CRYPTO, volume 403 of LNCS. Berlin: Springer: 1988. p. 94–99.)] continues to be the main contender in the space against factoring-based cryptosystems [[62](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR62" \o "Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978; 21(2):120–6.)], due to an underlying problem conjectured to be fully exponential in classical computers. Modern instantiations of ECC enjoy high performance and implementation simplicity and are very suited for embedded systems [[118](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR118" \o "Bernstein DJ. Curve25519: New diffie-hellman speed records. In: Public Key Cryptography. LNCS, 3958 vol.Berlin: Springer: 2006. p. 207–28.)–[120](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR120" \o )]. The dominance of number-theoretic primitives is however threatened by quantum computers as described in Section [3](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec6).

The plethora of new primitives must be rigorously evaluated from both the security and performance point of views, involving both theoretical work and engineering aspects. Implementations are expected to consume smaller amounts of energy [[121](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR121" \o "Banik S, Bogdanov A, Regazzoni F. Exploring energy efficiency of lightweight block ciphers. In: SAC. LNCS, 9566 vol.Berlin: Springer: 2015. p. 178–94.)], cycles and memory [[122](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR122" \o "Dinu D, Corre YL, Khovratovich D, Perrin L, Großschädl J, Biryukov A. Triathlon of lightweight block ciphers for the internet of things. NIST Workshop on Lightweight Cryptography. 2015.)] in ever decreasing devices and under more invasive attacks.

**Side-channel resistance**

If implemented without care, an otherwise secure cryptographic algorithm or protocol can leak critical information which may be useful to an attacker. Side-channel attacks [[123](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR123" \o "Kocher PC. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In: CRYPTO. LNCS, 1109 vol.Berlin: Springer: 1996. p. 104–13.)] are a significant threat against cryptography and may use timing information, cache latency, power and electromagnetic emanations to recover secret material. These attacks emerge from the interaction between the implementation and underlying computer architecture and represent an intrinsic security problem to pervasive computing environments, since the attacker is assumed to have physical access to at least some of the legitimate devices.

Protecting against intrusive side-channel attacks is a challenging research problem, and countermeasures typically promote some degree of regularity in computation. Isochronous or constant time implementations were among the first strategies to tackle this problem in the case of variances in execution time or latency in the memory hierarchy. The application of formal methods has enabled the first tools to verify isochronicity of implementations, such as information flow analysis [[124](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR124" \o "Rodrigues B, Pereira FMQ, Aranha DF. Sparse representation of implicit flows with applications to side-channel detection In: Zaks A, Hermenegildo MV, editors. Proceedings of the 25th International Conference on Compiler Construction, CC 2016, Barcelona, Spain, March 12-18, 2016. New York: ACM: 2016. p. 110–20.)] and program transformations [[125](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR125" \o "Almeida JB, Barbosa M, Barthe G, Dupressoir F, Emmi M. Verifying constant-time implementations. In: USENIX Security Symposium. Berkeley: USENIX Association: 2016. p. 53–70.)].

While there is a recent trend towards constructing and standardizing cryptographic algorithms with some embedded resistance against the simpler timing and power analysis attacks [[105](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR105" \o "Grosso V, Leurent G, Standaert F-X, Varici K. Ls-designs: Bitslice encryption for efficient masked software implementations. In: FSE. LNCS, 8540 vol.Berlin: Springer: 2014. p. 18–37.)], more powerful attacks such as differential power analysis [[126](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR126" \o "Kocher PC, Jaffe J, Jun B. Differential power analysis. In: CRYPTO. LNCS, 1666 vol. Springer: 1999. p. 388–97.)] or fault attacks [[127](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR127" \o "Biham E, Shamir A. Differential fault analysis of secret key cryptosystems. In: CRYPTO. LNCS, 1294 vol.Berlin: Springer: 1997. p. 513–25.)] are very hard to prevent or mitigate. Fault injection became a much more powerful attack methodology it was after demonstrated in software [[128](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR128" \o "Kim Y, Daly R, Kim J, Fallin C, Lee J-H, Lee D, Wilkerson C, Lai K, Mutlu O. Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. In: ISCA. Washington, DC: IEEE Computer Society: 2014. p. 361–72.)].

Masking techniques [[129](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR129" \o "Ishai Y, Sahai A, Wagner D. Private circuits: Securing hardware against probing attacks. In: CRYPTO. LNCS, 2729 vol. Springer: 2003. p. 463–81.)] are frequently investigated as a countermeasure to decorrelate leaked information from secret data, but frequently require robust entropy sources to achieve their goal. Randomness recycling techniques have been useful as a heuristic, but formal security analysis of such approaches is an open problem [[130](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR130" \o "Balasch J, Gierlichs B, Grosso V, Reparaz O, Standaert F-X. On the cost of lazy engineering for masked software implementations. In: CARDIS. LNCS, 8968 vol.Berlin: Springer: 2014. p. 64–81.)]. Modifications in the underlying architecture in terms of instruction set extensions, simplified execution environments and transactional mechanisms for restarting faulty computation are another promising research direction but may involve radical and possibly cost-prohibitive changes to current hardware.

**Resilience**

UbiComp relies on essential services as connectivity, routing and end-to-end communication. Advances in those essential services make possible the envisioned Weiser’s pervasive applications, which can count on transparent communication while reaching the expectations and requirements of final users in their daily activities. Among user’s expectations and requirements, the availability of services – not only communication services, but all services provided to users by UbiComp – is a paramount. Users more and more expect, and pay, for 24/7 available services. This is even more relevant when we think about critical UbiComp systems, such as those related to healthcare, urgency, and vehicular embedded systems.

Resilience is highlighted in this article, because it is one of the pillars of security. Resilience aims at identifying, preventing, detecting and responding to process or technological failures to recover or mitigate damages and financial losses resulted from service unavailability [[131](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR131" \o "Nogueira M, dos Santos AL, Pujolle G. A survey of survivability in mobile ad hoc networks. IEEE Commun Surv Tutor. 2009; 11(1):66–77.)]. In general, service unavailability has been associated with non-intentional failures, however, more and more the intentional exploitation of service availability breaches is becoming disruptive and out of control, as seen in the latest Distributed Denial of Service (DDoS) attack against the company DYN, a leading DNS provider, and the DDoS attack against the company OVH, the French website hosting giant [[132](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR132" \o "Mansfield-Devine S. The growth and evolution of ddos. Netw Secur. 2015; 2015(10):13–20.), [133](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR133" \o )]. The latter reached an intense volume of malicious traffic of approximately 1 TB/s, generated from a large amount of geographically distributed and infected devices, such as printers, IP cameras, residential gateways and baby monitors. Those devices are directly related to the modern concept of UbiComp systems [[134](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR134" \o )] and they intend to provide ubiquitous services to users.

However, what attracts the most the attention here is the negative side effect of the ubiquity exploitation against service availability. It is fact today that the Mark Weiser’s idea of *Computer for the 21st Century* has open doors to new kind of highly disruptive attacks. Those attacks are in general based on the idea of invisibility and unawareness for the devices in our homes, works, cities, and countries. But, exactly because of this, people seems to not pay enough attention to basic practices, such as change default passwords in Internet connect devices as CCTV cameras, baby monitors, smart TVs and other. This simple fact has been pointed as the main cause of the two DDoS attacks mentioned before and a report by global professional services company Deloitte suggests that Distributed Denial of Service (DDoS) attacks, that compromise exactly service availability, increased in size and scale in 2017, thanks in part to the growing multiverse of connected things.They also mentioned that DDoS attacks will be more frequent, with an estimated 10 million attacks in few months.

As there is no guarantee to completely avoid these attacks, resilient solutions become a way to mitigate damages and quickly resume the availability of services. Resilience is then necessary and complementary to the other solutions we observe in the previous sections of this article. Hence, this section focuses on highlighting the importance of resilience in the context of UbiComp systems. We overview the state-of-the-art regarding to resilience in the UbiComp systems and point out future directions for research and innovation [[135](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR135" \o "Santos AA, Nogueira M, Moura JMF. A stochastic adaptive model to explore mobile botnet dynamics. IEEE Commun Lett. 2017; 21(4):753–6.)–[138](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR138" \o "Lipa N, Mannes E, Santos A, Nogueira M. Firefly-inspired and robust time synchronization for cognitive radio ad hoc networks. Comput Commun. 2015; 66:36–44.)]. We also understand that resilience in these systems still requires a lot of investigations, however we believe that it was our role to raise this point to discussion through this article.

In order to contextualize resilience in the scope of UbiComp, it is important to observe that improvements on information and communication technologies, such as wireless networking, have increased the use of distributed systems in our everyday lives. Network access is becoming ubiquitous through portable devices and wireless communications, making people more and more dependent on them. This raising dependence claims for simultaneous high level of reliability and availability. The current networks are composed of heterogeneous portable devices, communicating among themselves generally in a wireless multi-hop manner [[139](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR139" \o "Zhang C, Song Y, Fang Y. Modeling secure connectivity of self-organized wireless ad hoc networks. In: IEEE INFOCOM. Piscataway: IEEE: 2008. p. 251–5.)]. These wireless networks can autonomously adapt to changes in their environment such as device position, traffic pattern and interference. Each device can dynamically reconfigure its topology, coverage and channel allocation in accordance with changes.

UbiComp poses nontrivial challenges to resilience design due to the characteristics of the current networks, such as shared wireless medium, highly dynamic network topology, multi-hop communication and low physical protection of portable devices [[140](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR140" \o "Salem NB, Hubaux J-P. Securing wireless mesh networks. IEEE Wirel Commun. 2006; 13(2):50–5.), [141](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR141" \o "Yang H, Luo H, Ye F, Lu S, Zhang L. Security in mobile ad hoc networks: challenges and solutions. IEEE Wirel Commun. 2004; 11(1):38–47.)]. Moreover, the absence of central entities in different scenarios increases the complexity of resilience management, particularly, when it is associated with access control, node authentication and cryptographic key distribution.

Network characteristics, as well as constraints on other kind of solutions against attacks that disrupt service availability, reinforce the fact that no network is totally immune to attacks and intrusions. Therefore, new approaches are required to promote the availability of network services. Such requirements motivate the design of resilient network services. In this work, we focus on the delivery of data from one UbiComp device to another as a fundamental network functionality and we emphasize three essential services: physical and link-layer connectivity, routing and end-to-end logical communication. However, resilience has also been observed under other perspectives. We follow the claim that resilience is achieved upon a cross-layer security solution that integrates preventive (i.e., cryptography and access control), reactive (i.e., intrusion detection systems) and tolerant (i.e., packet redundancy) defense lines in a self-adaptive and coordinated way [[131](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR131" \o "Nogueira M, dos Santos AL, Pujolle G. A survey of survivability in mobile ad hoc networks. IEEE Commun Surv Tutor. 2009; 11(1):66–77.), [142](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR142" \o "Nogueira M. SAMNAR: A survivable architecture for wireless self-organizing networks. PhD thesis, Université Pierre et Marie Curie - LIP6. 2009.)].

However, what are still the open challenges to achieve resilience in the UbiComp context? First of all, we emphasize the heterogeneity of devices and technologies that compose UbiComp environments. The integration from large-scale systems, such as Cloud data centers, to tiny devices, such as wearable and implantable sensors, is a huge challenge itself due to the complexity resulted from it. Then, in addition, providing integration of preventive, reactive and tolerant solutions and their adaptation is even harder in face of the different requirements of these devices, their capabilities in terms of memory and processing, and application requirements. Further, dealing with heterogeneity in terms of communication technology and protocols makes challenging the analysis of network behavior and topologies, what in conventional systems are employed to assist in the design of resilient solutions.

Another challenge is how to deal with scale. First, the UbiComp systems tend to be hyper-scale and geographically distributed. How to cope, then, with the complexity resulted from that? How to define and construct models to understand these systems and offer resilient services? Finally, we also point out as challenges the uncertainty and speed. If on the one hand, it is so hard to model, analyze and define resilient services in this complex system, on the other hand uncertainly is a norm on them, being speed and low response time a strong requirement for the applications in these systems. Hence, how to address all these elements together? How to manage them in order to offer resilient services considering diverse kind of requirements from the various applications?

All these questions lead to deep investigation and challenges. However, they also show opportunities for applied research in designing and engineering resilient systems, mainly for the UbiComp context. Particularly, if we advocate for designing resilient systems that manage the three defense lines in an adaptive way. We believe that this management can promote a great advance for applied research and for resilience.

**Privacy implications**

UbiComp systems tend to collect a lot of data and generate a lot of information. Correctly used, information generates innumerable benefits to our society that has provided us with a better life over the years. However, the information can be used for illicit purposes, just as computer systems are used for attacks. Protecting private information is a great challenge that can often seem impractical, for instance, protecting customers’ electrical consumption data from their electricity distribution company [[184](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR184" \o "Borges F, Demirel D, Bock L, Buchmann JA, Mühlhäuser M. A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In: ISCC. USA: IEEE: 2014. p. 1–6.)–[186](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR186" \o "Borges de Oliveira F. Reasons to Measure Frequently and Their Requirements. Cham: Springer International Publishing; 2017. p. 39–47.)].

Ensuring security is a necessary condition for ensuring privacy, for instance, if the communication between clients and a service provider is not secure, then privacy is not guaranteed. However, it is not a sufficient condition, for instance, the communication is secure, but a service provider uses the data in a not allowed way. We can use cryptography to ensure secure as well as privacy. Nevertheless, even though one uses encrypted communication, the metadata from the network traffic might reveal private information. The first challenge is to find the extend of the data relevance and the impact of data leakage.

**Application scenario challenges**

Finding which data might be sensitive is a challenging task. Some cultures classify some data as sensitive when others classify the same data as public. Another challenge is to handle regulations from different countries.

**Identifying sensitive data**

Classifying what may be sensitive data might be a challenging task. The article 12 of the Universal Declaration of Human Rights proclaimed by the United Nations General Assembly in Paris on 10 December 1948 states: No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. Lawmakers have improved privacy laws around the world. However, there is still plenty of room for improvements, specially, when we consider data from people, animals, and products. Providers can use such data to profile and manipulate people and market. Unfair competitors might use private industrial data to get advantages over other industries.

**Regulation**

UbiComp systems tend to run worldwide. Thus, their developers need to deal with several laws from distinct cultures. The abundance of laws is a challenge for international institutions. The absence of laws too. On the one hand, the excess of laws compels institutions to handle a huge bureaucracy to follow several laws. On the other hand, the absence of laws causes unfair competition because unethical companies can use private data to get advantages over ethical companies. Business models must use privacy-preserving protocols to ensure democracy and avoid a surveillance society (see [[187](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR187" \o "Holvast J. The Future of Identity in the Information Society, volume 298 of IFIP Advances in Information and Communication Technology In: Matyáš V, Fischer-Hübner S, Cvrček D, Švenda P, editors. Berlin: Springer Berlin Heidelberg: 2009. p. 13–42.)]). Such protocols are the solution for the dilemma between privacy and information. However, they have their own technological challenges.

**Technological challenges**

We can deal with already collected data from legacy systems or private-by-design data that are collected by privacy-preserving protocols, for instance, databases used in old systems and messages from privacy-preserving protocols, respectively. If a scenario can be classified as both, we can just tackle it as an already collected data in the short term.

**Already collected data**

One may use a dataset for information retrieval while keeping the anonymity of the true owners’ data. One may use data mining techniques over a private dataset. Several techniques are used in privacy preserving data mining [[188](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR188" \o "Toshniwal D. Privacy preserving data mining techniques privacy preserving data mining techniques for hiding sensitive data hiding sensitive data: a step towards open data open data. Singapore: Springer Singapore: 2018. p. 205–12.)]. ARX Data Anonymization Tool is a very interesting tool for anonymization of already collected data. In the following, we present several techniques used to provide privacy in already collected data.

**Anonymization**

Currently, we have several techniques for anonymization and to evaluate the level of anonymization, for instance, *k*-anonymity, *l*-diversity, and *t*-closeness [[189](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR189" \o "Li N, Li T, Venkatasubramanian S. t-closeness: Privacy beyond k-anonymity and l-diversity. In: 2007 IEEE 23rd International Conference on Data Engineering. USA: IEEE: 2007. p. 106–15.)]. They use a set *E* from data indistinguishable for an identifier in a table.

The method *k*-anonymity suppresses table columns or replace them for keeping each *E* with at least *k* registers. It seems safe, but only 4 points marking the position on the time are enough to identify uniquely 95% of the cellphone users [[190](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR190" \o "De Montjoye Y-A, Hidalgo CA, Verleysen M, Blondel VD. Unique in the crowd: The privacy bounds of human mobility. Sci Rep. 2013; 3:1–5.)].

The method *l*-diversity requires that each *E* have at least *l* values “well-represented” for each sensitive column. Well-represented can be defined in three ways:

1. at least l distinct values for each sensitive column;

2. for each E, the Shannon entropy is limited, such that H(E)⩾log2lH(E)⩾log2⁡l, where H(E)=−∑s∈SPr(E,s)log2(Pr(E,s)),H(E)=−∑s∈SPr(E,s)log2⁡(Pr(E,s)),S is the domain of the sensitive column, and Pr(E,s) is the probability of the lines in E that have sensitive values s;

1. the most common values cannot appear frequently, and the most uncommon values cannot appear infrequently.

Note that some tables do not have l distinct sensitive values. Furthermore, the table entropy should be at least log2l. Moreover, the frequency of common and uncommand values usually are not close to each other.

We say that E is t-closeness if the distance between the distribution of a sensitive column E end the distribution of column in all the table is not more than a threshold t. Thus, we say that a table has t-closeness if every E in a table have t-closeness. In this case, the method generates a trade-off between data usefulness and privacy.

**Differential privacy**

The idea of differential privacy is similar to the idea of indistinguishability in cryptography. For defining it, let *ε* be a positive real number and AA be a probabilistic algorithm with a dataset as input. We say that AA is *ε*-differentially private if for every dataset *D*1 and *D*2 that differ in one element, and for every subset *S* of the image of AA, we have Pr[A(*D*1)∈*S*]≤*eϵ*×Pr[A(*D*2)∈ *S*],Pr[A(D1)∈S]≤eϵ×Pr[A(D2)∈ S], where the probability is controlled for the algorithm randomness.

Differential privacy is not a metric in the mathematical sense. However, if the algorithms keep the probabilities based on the input, we can construct a metric d to compare the distance between two algorithms with d(A1,A2)=|ϵ1−ϵ2|.d(A1,A2)=|ϵ1−ϵ2|. In this way, we can determine if two algorithms as equivalents ε1=ε2, and we can determine the distance from an ideal algorithm computing d(A1,Aideal)=|ϵ1−0|.

**Entropy and the degree of anonymity**

The degree of anonymity g can be measured with the Shannon entropy H(X)=∑Ni=1[pi⋅log2(1pi)],H(X)=∑i=1N[pi⋅log2⁡(1pi)], where H(X) is the network entropy, N is the number of nodes, and pi is the probability for each node i. The maximal entropy happens when the probability is uniform, i.e., all nodes are equiprobably 1/N, hence HM= log2(N). Therefore, the anonymity degree g is defined by g=1−HM−H(X)HM=H(X)HM.g=1−HM−H(X)HM=H(X)HM.

Similar to differential privacy, we can construct a metric to compare the distance between two networks computing d(g1,g2)=|g1−g2|. Similarly, we can compare if they are equivalent g1=g2. Thus, we can determine the distance from an ideal anonymity network computing d(g1,gideal)=|g1−1|.

The network can be replaced by a dataset, but in this model, each register should have a probability.

**Complexity**

Complexity analysis also can be used as a metric to measure the time required in the best case for retrieving information from an anonymized dataset. It can also be used in private-by-design data as the time required to break a privacy-preserving protocol. The time measure can be done with asymptotical analysis or counting the number of steps to break the method.

All techniques have their advantages and disadvantages. However, even though the complexity prevents the leakage, even though the algorithm has differential privacy, even though the degree of anonymity is the maximum, privacy might be violated. For example, in an election with 3 voters, if 2 collude, then the third voters will have the privacy violated independent of the algorithm used. In [[191](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR191" \o "Borges de Oliveira F. Quantifying the aggregation size. Cham: Springer International Publishing; 2017. p. 49–60.)], we find how to break protocols based on noise for smart grids, even when they are provided with the property of differential privacy.

Cryptography should ensure privacy in the same way that ensures security. An encrypted message should have maximum privacy metrics as well as cryptography ensures for security. We should use the best algorithm that leaks privacy and compute its worst-case complexity.

**Probability**

We can use probabilities to measure the chances of leakage. This approach is independent of algorithm used to protect privacy.

For example, consider an election with 3 voters. If 2 voters cast yes and 1 voter cast no, an attacker knows that the probability of a voter cast yes is 2/3 and for no is 1/3. The same logics applies if the number of voters and candidates grow.

Different from the case of yes and no, we may keep the privacy from valued measured. For attackers to discover the time series of three points, they represent each point for a number of stars, i.e., symbols ⋆. Thus, attackers can split the total number of stars in three boxes. Let the sum of the series be 7, a probability would be ⋆⋆⋆⋆ ⋆ ⋆⋆. For simplicity, attackers can split the stars by bars instead of boxes. Hence, ⋆⋆⋆⋆ |⋆|⋆⋆ is the same solution. With such notation, the binomial of 7 stars plus 2 bars chosen 7 stars determines the possible number of solutions, i.e., (7+27)=9!7!(9−7)!=36.(7+27)=9!7!(9−7)!=36.

Generalizing, if *t* is the number of points in a time series and *s* its sum, then the number of possible time series for the attackers to decide the correct is determined by *s* plus *t*−1 chosen *s*, i.e.,

(*s*+*t*−1*s*)=(*s*+*t*−1)!(*t*−1)!*s*!=(*s*+*t*−1*i*−1).(s+t−1s)=(s+t−1)!(t−1)!s!=(s+t−1i−1).

(1)

If we collect multiple time series, we can form a table, e.g., a list of candidates with the number of votes by states. The tallyman cold reveal only the total number of voter by state and the total number of votes by candidate, who could infer the possible number of votes by state [[191](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR191" \o "Borges de Oliveira F. Quantifying the aggregation size. Cham: Springer International Publishing; 2017. p. 49–60.)]. Data from previous elections may help the estimation. The result of the election could be computed over encrypted data in a much more secure way than anonymization by *k*-anonymity, *l*-diversity, and *t*-closeness. Still, depending on the size of the table and its values, the time series can be found.

In general, we can consider measurements instead of values. Anonymity techniques try to reduce the number of measurements in the table. Counterintuitively, smaller the number of measurements, bigger the chances of discover them [[191](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR191" \o "Borges de Oliveira F. Quantifying the aggregation size. Cham: Springer International Publishing; 2017. p. 49–60.)].

If we consider privacy by design, we do not have already collected data.

**Private-by-design data**

Messages is the common word for private-by-design data. Messages are transmitted data, processed, and stored. For privacy-preserving protocols, individual messages should not be leaked. CryptDB is an interesting tool, which allows us to make queries over encrypted datasets. Although messages are stored in a dataset, they are encrypted messages with the users’ keys. To keep performance reasonable, privacy-preserving protocols aggregate or consolidate messages and solve a specific problem.

**Computing all operators**

In theory, we can compute a Turin machine over encrypted data, i.e., we can use a technique called fully homomorphic encryption [[192](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR192" \o "Gentry C. A Fully Homomorphic Encryption Scheme. Stanford: Stanford University; 2009. AAI3382729.)] to compute any operator over encrypted data. The big challenge of fully homomorphic encryption is performance. Hence, constructing a fully homomorphic encryption for many application scenarios is a herculean task. The most usual operation is addition. Thus, most privacy-preserving protocols use additive homomorphic encryption [[193](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR193" \o "Borges de Oliveira F. A Selective Review. Cham: Springer International Publishing; 2017. p. 25–36.)] and DC-Nets (from “Dining Cryptographers”) [[194](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR194" \o "Borges de Oliveira F. Selected Privacy-Preserving Protocols. Cham: Springer International Publishing; 2017. p. 61–100.)]. Independent of the operation, the former generates functions, and the latter generates families of functions. We can construct an asymmetric DC-Net based on an additive homomorphic encryption [[194](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR194" \o "Borges de Oliveira F. Selected Privacy-Preserving Protocols. Cham: Springer International Publishing; 2017. p. 61–100.)].

**Trade-off between enforcement and malleability**

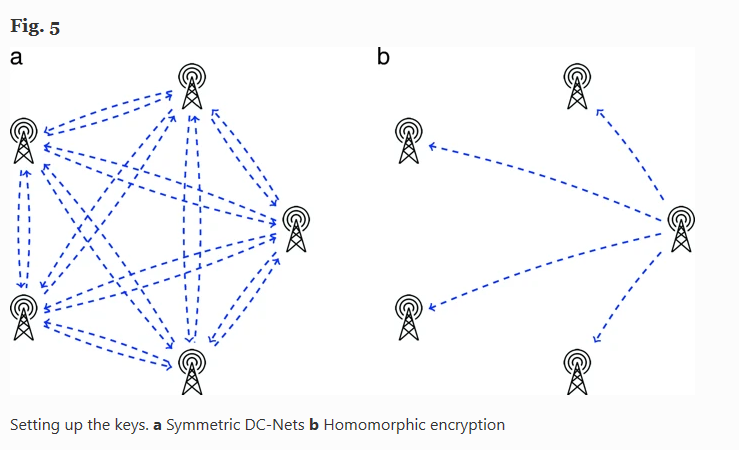
The privacy enforcement has a high cost. With DC-Nets, we can enforce privacy. However, every encrypted message need to be considered in the computation for users to decrypt and to access the protocol output. It is good for privacy but bad for fault tolerance. For illustration, consider an election where all voters need to vote. Homomorphic encryption enables protocols to decrypt and output even missing an encrypted message. Indeed, it enables the decryption of a single encrypted message. Therefore, homomorphic encryption cannot ensure privacy. For illustration, consider an election where one can read and change all votes. Homomorphic encryption techniques are malleable, and DC-Nets are non-malleable. On the one hand, mailability simplifies the process and improve fault tolerance but disables privacy enforcement. On the other hand, non-mailability enforces privacy but complicates the process and diminishes fault tolerance. In addition, the key distribution with homomorphic encryption is easier than with DC-Net schemes.

**Key distribution**

Homomorphic encryption needs a public-private key pair. Who owns the private key controls all the information. Assume that a receiver generates the key pair and send the public key to the senders in a secure communication channel. Thus, senders will use the same key to encrypt their messages. Since homomorphic encryption schemes are probabilistic, sender can use the same key to encrypt the same message that their encrypted messages will be different from each other. However, the receiver does not know who sent the encrypted messages.

DC-Net needs a private key for each user and a public key for the protocol. Since DC-Nets do not require senders and receiver, the users are usually named participants. They generate their own private key. Practical symmetric DC-Nets need that participants send a key to each other in a secure communication channel. Afterward, each participant has a private key given by the list of shared keys. Hence, each participant encrypts computing Mi,j←Enc(mi,j)=mi,j+∑o∈M−{i}Hash(si,o || j)−Hash(so,i || j),Mi,j←Enc(mi,j)=mi,j+∑o∈M−{i}Hash(si,o || j)−Hash(so,i || j), where mi,j is the message sent by the participant i in the time j, Hash is a secure hash function predefined by the participants, si,o is the secret key sent from participant i to participant o, similarly, so,i is the secret key received by i from o, and || is the concatenation operator. Each participant i can send the encrypted message Mi,jMi,j to each other. Thus, participants can decrypt the aggregated encrypted messages computing Dec=∑i∈MMi,j=∑i∈Mmi,j.Dec=∑i∈MMi,j=∑i∈Mmi,j. Note that if one or more messages are missing, the decryption is infeasible. Asymmetric DC-Nets do not require a private key based on shared keys. Each participant simply generates a private key. Subsequently, they use a homomorphic encryption or a symmetric DC-Net to add their private keys generating the decryption key.

Homomorphic encryption schemes have low overhead than DC-Nets for setting up keys and for distributing them. Symmetric DC-Nets need O(I2) messages to set up the keys, where I is the number of participants. Figure [5](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig5) depicts the messages to set up keys using (a) symmetric DC-Nets and (b) homomorphic encryption. Asymmetric DC-Nets can be settled easier than symmetric DC-Nets with the price of trusting the homomorphic encryption scheme.



**Aggregation and consolidation**

The aggregation and consolidation with DC-Nets are easier than with homomorphic encryption. Using DC-Nets, participants can just broadcast their encrypted messages or just send directly to an aggregator. Using homomorphic encryption, senders cannot send encrypted messages directly to the receiver, who can decrypt individual messages. Somehow, senders should aggregate the encrypted messages, and the receiver should receive only the encrypted aggregation, which is a challenge in homomorphic encryption and trivial in DC-Nets due to the trade-off described in Section [7.4.2](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Sec34). In this work, we are referencing DC-Nets as fully connected DC-Nets. For non-fully connected DC-Nets, aggregation is based on trust and generates new challenges. Sometimes, aggregation and consolidation are used as synonym. However, consolidation is more complicated and generates more elaborate information than the aggregation. For example, the aggregation of the encrypted textual messages is just to join them, while the consolidation of encrypted textual messages generates a speech synthesis.

**Performance**

Fully homomorphic encryption tends to have big keys and requires a prohibitive processing time. On the contrary, asymmetric DC-Nets and partially homomorphic encryption normally use modular multi-exponentiations, which can be computed in logarithmic time [[195](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR195" \o "Borges F, Lara P, Portugal R. Parallel algorithms for modular multi-exponentiation. Appl Math Comput. 2017; 292:406–16.)]. Symmetric DC-Nets are efficient only for a small number of participants, because each participant need an iteration over the number of participants to encrypt a message. The number of participants is not relevant for asymmetric DC-Nets and for homomorphic encryption.

**Forensics**

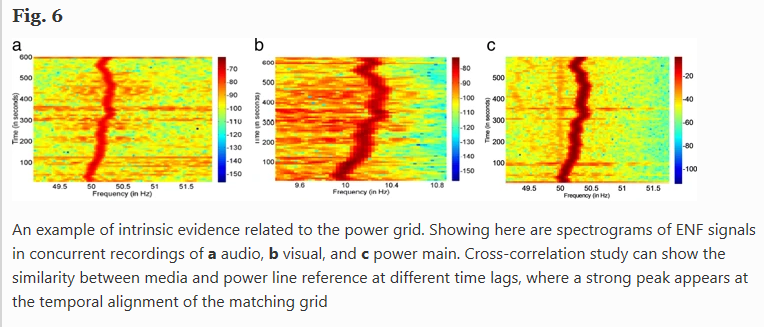
Digital forensics is a branch of forensic science addressing the recovery and investigation of material found in digital devices. Evidence collection and interpretation play a key role in forensics. Conventional forensic approaches separately address issues related to computer forensics and information forensics. There is, however, a growing trend in security and forensics research that utilizes interdisciplinary approaches to provide a rich set of forensic capabilities to facilitate the authentication of data as well as the access conditions including who, when, where, and how.

In this trend, there are two major types of forensic evidences [[196](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR196" \o "Stamm MC, Wu M, Liu KJR. Information forensics: An overview of the first decade. IEEE Access. 2013; 1:167–200.)]. One type is intrinsic to the device, the information processing chain, or the physical environment, in such forms as the special characteristics associated with specific types of hardware or software processing or environment, the unique noise patterns as a signature of a specific device unit, certain regularities or correlations related to certain device, processing or their combinations, and more. Another type is extrinsic approaches, whereby specially designed data are proactively injected into the signals/data or into the physical world and later extracted and examined to infer or verify the hosting data’s origin, integrity, processing history, or capturing environment.

In mid of the convergence between digital and physical systems with sensors, actuators and computing devices becoming closely tied together, an emerging framework has been proposed as Proof-Carrying Sensing (PCS) [[197](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR197" \o "Wu M, Quintão Pereira FM, Liu J, Ramos HS, Alvim MS, Oliveira LB. New directions: Proof-carrying sensing — Towards real-world authentication in cyber-physical systems. In: Proceedings of ACM Conf. on Embedded Networked Sensor Systems (SenSys). New York: ACM: 2017.)]. This was inspired by Proof-Carrying Code, a trusted computing framework that associates foreign executables with a model to prove that they have not been tampered with and they function as expected. In the new UbiComp context involving cyber physical systems where mobility and resource constraints are common, the physical world can be leveraged as a channel that encapsulates properties difficult to be tampered with remotely, such as proximity and causality, in order to create a challenge-response function. Such a Proof-Carrying Sensing framework can help authenticate devices, collected data, and locations, and compared to traditional multifactor or out-of-band authentication mechanisms, it has a unique advantage that authentication proofs are embedded in sensor data and can be continuously validated over time and space at without running complicated cryptographic algorithms.

In terms of the above-mentioned intrinsic and extrinsic view point, the physical data available to establish a mutual trust in the PCS framework can be intrinsic to the physical environment (such as temperature, luminosity, noise, electrical frequency), or extrinsic to it, for example, they are actively injected by the device into the physical world. By monitoring the propagation of intrinsic or extrinsic data, a device can confirm its reception by other devices located within its vicinity. The challenge in designing and securely implementing such protocols can be addressed by the synergy of combined expertises such as signal processing, statistical detection and learning, cryptography, software engineering, and electronics.

To help appreciate the intrinsic and extrinsic evidences in addressing the security and forensics in UbiComp that involves both digital and physical elements, we now discuss two examples. Consider first an intrinsic signature of power grids. The electric network frequency (ENF) is the supply frequency of power distribution grids, with a nominal value of 60Hz (North America) or 50Hz (Europe). At any given time, the instantaneous value of ENF usually fluctuates around its nominal value as a result of the dynamic interaction between the load variations in the grid and the control mechanisms for power generation. These variations are nearly identical in all locations of the same grid at a given time due to the interconnected nature of the grid. The changing values of instantaneous ENF over time forms an ENF signal, which can be intrinsically captured by audio/visual recordings (Fig. [6](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "Fig6)) or other sensors [[198](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR198" \o "Grigoras C. Applications of ENF analysis in forensic authentication of digital audio and video recordings. J Audio Eng Soc. 2009; 57(9):643–61.), [199](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR199" \o "Garg R, Varna AL, Hajj-Ahmad A, Wu M. \“seeing\” enf: Power-signature-based timestamp for digital multimedia via optical sensing and signal processing. TIFS. 2013; 8(9):1417–32.)]. This has led to recent forensic applications, such as validating the time-of-recording of an ENF-containing multimedia signal and estimating its recording location using concurrent reference signals from power grids based on the use of ENF signals.



Next, consider the recent work by Satchidanandan and Kumar [[200](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR200" \o "Satchidanandan B, Kumar PR. Dynamic watermarking: Active defense of networked cyber–physical systems. Proc IEEE. 2017; 105(2):219–40.)] introducing a notion of watermarking in a cyber-physical system, which can be viewed as a class of extrinsic signatures. If an actuator injects into the system a properly designed probing signal that is unknown in advance to other nodes in the system, then based on the knowledge of the cyber-physical system’s dynamics and other properties, the actuator can examine the sensors’ report about the signals at various points and can potentially infer whether there is malicious activity in the system or not, and if so, where and how.

A major challenge and research opportunity lies on discovering and characterizing suitable intrinsic and extrinsic evidences. Although qualitative properties of some signatures are known, it is important to develop quantitative models to characterize the normal and abnormal behavior in the context of the overall system. Along this line, the exploration of physical models might yield analytic approximations of such properties; and in the meantime, data-driven learning approaches can be used to gather statistical data characterizing normal and abnormal behaviors. Building on these elements, a strong synergy across the boundaries of traditionally separate domains of computer forensics, information forensics, and device forensics should be developed so as to achieve comprehensive capabilities of system forensics in UbiComp.

**Conclusion**

In the words of Mark Weiser, Ubiquitous Computing is “the idea of integrating computers seamlessly into the world at large” [[1](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "ref-CR1" \o "Weiser M. The computer for the 21st century. Sci Am. 1991; 265(3):94–104.)]. Thus, far from being a phenomenon from this time, the design and practice of UbiComp systems were already being discussed one quarter of a century ago. In this article, we have revisited this notion, which permeates the most varied levels of our society, under a security and privacy point of view. In the coming years, these two topics will occupy much of the time of researchers and engineers. In our opinion, the use of this time should be guided by a few observations, which we list below:

* UbiComp software is often produced as the combination of different programming languages, sharing a common core often implemented in a type-unsafe language such as C, C++ or assembly. Applications built in this domain tend to be distributed, and their analysis, i.e., via static analysis tools, needs to consider a holistic view of the system.
* The long-life span of some of these systems, coupled with the difficulty (both operational and cost-wise) to update and re-deploy them, makes them vulnerable to the inexorable progress of technology and cryptanalysis techniques. This brings new (and possibly disruptive) players to this discussion, such as quantum adversaries.
* Key management is a critical component of any secure or private real-world system. After security roles and key management procedures are clearly defined for all entities in the framework, a set of matching cryptographic primitives must be deployed. Physical access and constrained resources complicate the design of efficient and secure cryptographic algorithms, which are often amenable to side-channel attacks. Hence, current research challenges in the space include more efficient key management schemes, in particular supporting some form of revocation; the design of lightweight cryptographic primitives which facilitate correct and secure implementation; cheaper side-channel resistance countermeasures made available through advances in algorithms and embedded architectures.
* Given the increasing popularization of UbiComp systems, people become more and more dependent on their services for performing different commercial, financial, medical and social transactions. This rising dependence requires simultaneous high level of reliability, availability and security. This observation strengthens the importance of the design and implementation of resilient UbiComp systems.
* One of the main challenges to providing pervasive IdM is to ensure the authenticity of devices and users and adaptive authorization in scenarios with multiple and heterogeneous security domains.
* Several databases currently store sensitive data. Moreover, a vast number of sensors are constantly collecting new sensitive data and storing them in clouds. Privacy-preserving protocols are being designed and perfected to enhance user’s privacy in specific scenarios. Cultural interpretations of privacy, the variety of laws, big data from legacy systems in clouds, processing time, latency, key distribution and management, among other aforementioned are challenges for us to develop privacy-preserving protocols.
* The convergence between the physical and digital systems poses both challenges and opportunities in offering forensic capabilities to facilitate the authentication of data as well as the access conditions including who, when, where, and how; a synergistic use of intrinsic and extrinsic evidences with interdisciplinary expertise will be the key.

Given these observations, and the importance of ubiquitous computing, it is easy to conclude that the future holds fascinating challenges waiting for the attention of the academia and the industry.

Finally, note the observations and the predictions presented in this work regarding how UbiComp may evolve represent our view of the field based on the technology landscape today. New scientific discoveries, technology inventions as well as economic, social, and policy factors may lead to new and/or different trends in the technology evolutionary paths.

**Reference**

1.Weiser M. The computer for the 21st century. Sci Am. 1991; 265(3):94–104.

[Article](https://doi.org/10.1038/scientificamerican0991-94)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=The computer for the 21st century&journal=Sci Am&volume=265&issue=3&pages=94-104&publication_year=1991&author=Weiser,M)

2.Weiser M. Some computer science issues in ubiquitous computing. Commun ACM. 1993; 36(7):75–84.

[Article](https://doi.org/10.1145/159544.159617)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Some computer science issues in ubiquitous computing&journal=Commun ACM&volume=36&issue=7&pages=75-84&publication_year=1993&author=Weiser,M)

3.Lyytinen K, Yoo Y. Ubiquitous computing. Commun ACM. 2002; 45(12):63–96.

[Article](https://doi.org/10.1145/585597.585616)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Ubiquitous computing&journal=Commun ACM&volume=45&issue=12&pages=63-96&publication_year=2002&author=Lyytinen,K&author=Yoo,Y)

4.Estrin D, Govindan R, Heidemann JS, Kumar S. Next century challenges: Scalable coordination in sensor networks. In: MobiCom’99. New York: ACM: 1999. p. 263–70.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=MobiCom%E2%80%9999&publication_year=1999&author=Estrin,D&author=Govindan,R&author=Heidemann,JS&author=Kumar,S)

5.Pottie GJ, Kaiser WJ. Wireless integrated network sensors. Commun ACM. 2000; 43(5):51–8.

[Article](https://doi.org/10.1145/332833.332838)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Wireless integrated network sensors&journal=Commun ACM&volume=43&issue=5&pages=51-8&publication_year=2000&author=Pottie,GJ&author=Kaiser,WJ)

6.Ashton K. That ’Internet of Things’ Thing. RFiD J. 2009; 22:97–114.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=That %E2%80%99Internet of Things%E2%80%99 Thing&journal=RFiD J&volume=22&pages=97-114&publication_year=2009&author=Ashton,K)

7.Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput Netw. 2010; 54(15):2787–805.

[MATH](http://www.emis.de/MATH-item?1208.68071)

[Article](https://doi.org/10.1016/j.comnet.2010.05.010)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=The internet of things: a survey&journal=Comput Netw&volume=54&issue=15&pages=2787-805&publication_year=2010&author=Atzori,L&author=Iera,A&author=Morabito,G)

8.Mann S. Wearable computing: A first step toward personal imaging. Computer. 1997; 30(2):25–32.

[Article](https://doi.org/10.1109/2.566147)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Wearable computing: A first step toward personal imaging&journal=Computer&volume=30&issue=2&pages=25-32&publication_year=1997&author=Mann,S)

9.Martin T, Healey J. 2006’s wearable computing advances and fashions. IEEE Pervasive Comput. 2007; 6(1):14–6.

[Article](https://doi.org/10.1109/MPRV.2007.2)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=2006%E2%80%99s wearable computing advances and fashions&journal=IEEE Pervasive Comput&volume=6&issue=1&pages=14-6&publication_year=2007&author=Martin,T&author=Healey,J)

10.Lee EA. Cyber-physical systems-are computing foundations adequate. In: NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, volume 2. Citeseer: 2006.

11.Rajkumar RR, Lee I, Sha L, Stankovic J. Cyber-physical systems: the next computing revolution. In: 47th Design Automation Conference. ACM: 2010.

12.Abowd GD, Mynatt ED. Charting past, present, and future research in ubiquitous computing. ACM Trans Comput Human Interact (TOCHI). 2000; 7(1):29–58.

[Article](https://doi.org/10.1145/344949.344988)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Charting past, present, and future research in ubiquitous computing&journal=ACM Trans Comput Human Interact (TOCHI)&volume=7&issue=1&pages=29-58&publication_year=2000&author=Abowd,GD&author=Mynatt,ED)

13.Stajano F. Security for ubiquitous computing.Hoboken: Wiley; 2002.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Security for ubiquitous computing.&publication_year=2002&author=Stajano,F)

14.Pierce BC. Types and programming languages, 1st edition. Cambridge: The MIT Press; 2002.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Types and programming languages&publication_year=2002&author=Pierce,BC)

15.Cousot P, Cousot R. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In: POPL. New York: ACM: 1977. p. 238–52.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=POPL&publication_year=1977&author=Cousot,P&author=Cousot,R)

16.McMillan KL. Symbolic model checking. Norwell: Kluwer Academic Publishers; 1993.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Symbolic model checking&publication_year=1993&author=McMillan,KL)

17.Leroy X. Formal verification of a realistic compiler. Commun ACM. 2009; 52(7):107–15.

[Article](https://doi.org/10.1145/1538788.1538814)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Formal verification of a realistic compiler&journal=Commun ACM&volume=52&issue=7&pages=107-15&publication_year=2009&author=Leroy,X)

18.Rice HG. Classes of recursively enumerable sets and their decision problems. Trans Amer Math Soc. 1953; 74(1):358–66.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=53041)

[MATH](http://www.emis.de/MATH-item?0053.00301)

[Article](https://doi.org/10.1090/S0002-9947-1953-0053041-6)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Classes of recursively enumerable sets and their decision problems&journal=Trans Amer Math Soc&volume=74&issue=1&pages=358-66&publication_year=1953&author=Rice,HG)

19.Wilson RP, Lam MS. Efficient context-sensitive pointer analysis for c programs. In: PLDI. New York: ACM: 1995. p. 1–12.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=PLDI&publication_year=1995&author=Wilson,RP&author=Lam,MS)

20.Cadar C, Dunbar D, Engler D. KLEE: Unassisted and automatic generation of high-coverage tests for complex systems programs. In: OSDI. Berkeley: USENIX: 2008. p. 209–24.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=OSDI&publication_year=2008&author=Cadar,C&author=Dunbar,D&author=Engler,D)

21.Coppa E, Demetrescu C, Finocchi I. Input-sensitive profiling. In: PLDI. New York: ACM: 2012. p. 89–98.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=PLDI&publication_year=2012&author=Coppa,E&author=Demetrescu,C&author=Finocchi,I)

22.Graham SL, Kessler PB, McKusick MK. gprof: a call graph execution profiler (with retrospective). In: Best of PLDI. New York: ACM: 1982. p. 49–57.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Best of PLDI&publication_year=1982&author=Graham,SL&author=Kessler,PB&author=McKusick,MK)

23.Godefroid P, Klarlund N, Sen K. Dart: directed automated random testing. In: PLDI. New York: ACM: 2005. p. 213–23.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=PLDI&publication_year=2005&author=Godefroid,P&author=Klarlund,N&author=Sen,K)

24.Nethercote N, Seward J. Valgrind: a framework for heavyweight dynamic binary instrumentation. In: PLDI. New York: ACM: 2007. p. 89–100.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=PLDI&publication_year=2007&author=Nethercote,N&author=Seward,J)

25.Luk C-K, Cohn R, Muth R, Patil H, Klauser A, Lowney G, Wallace S, Reddi VJ, Hazelwood K. Pin: Building customized program analysis tools with dynamic instrumentation. In: PLDI. New York: ACM: 2005. p. 190–200.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=PLDI&publication_year=2005&author=Luk,C-K&author=Cohn,R&author=Muth,R&author=Patil,H&author=Klauser,A&author=Lowney,G&author=Wallace,S&author=Reddi,VJ&author=Hazelwood,K)

26.Rimsa AA, D’Amorim M, Pereira FMQ. Tainted flow analysis on e-SSA-form programs. In: CC. Berlin: Springer: 2011. p. 124–43.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CC&publication_year=2011&author=Rimsa,AA&author=D%E2%80%99Amorim,M&author=Pereira,FMQ)

27.Serebryany K, Bruening D, Potapenko A, Vyukov D. Addresssanitizer: a fast address sanity checker. In: ATC. Berkeley: USENIX: 2012. p. 28.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ATC&publication_year=2012&author=Serebryany,K&author=Bruening,D&author=Potapenko,A&author=Vyukov,D)

28.Russo A, Sabelfeld A. Dynamic vs. static flow-sensitive security analysis. In: CSF. Washington: IEEE: 2010. p. 186–99.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CSF&publication_year=2010&author=Russo,A&author=Sabelfeld,A)

29.Carlini N, Barresi A, Payer M, Wagner D, Gross TR. Control-flow bending: On the effectiveness of control-flow integrity. In: SEC. Berkeley: USENIX: 2015. p. 161–76.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=SEC&publication_year=2015&author=Carlini,N&author=Barresi,A&author=Payer,M&author=Wagner,D&author=Gross,TR)

30.Klein G, Elphinstone K, Heiser G, Andronick J, Cock D, Derrin P, Elkaduwe D, Engelhardt K, Kolanski R, Norrish M, Sewell T, Tuch H, Winwood S. sel4: Formal verification of an os kernel. In: SOSP. New York: ACM: 2009. p. 207–20.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=SOSP&publication_year=2009&author=Klein,G&author=Elphinstone,K&author=Heiser,G&author=Andronick,J&author=Cock,D&author=Derrin,P&author=Elkaduwe,D&author=Engelhardt,K&author=Kolanski,R&author=Norrish,M&author=Sewell,T&author=Tuch,H&author=Winwood,S)

31.Jourdan J-H, Laporte V, Blazy S, Leroy X, Pichardie D. A formally-verified c static analyzer. In: POPL. New York: ACM: 2015. p. 247–59.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=POPL&publication_year=2015&author=Jourdan,J-H&author=Laporte,V&author=Blazy,S&author=Leroy,X&author=Pichardie,D)

32.Soares LFG, Rodrigues RF, Moreno MF. Ginga-NCL: the declarative environment of the brazilian digital tv system. J Braz Comp Soc. 2007; 12(4):1–10.

[Article](https://doi.org/10.1590/S0104-65002007000100005)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Ginga-NCL: the declarative environment of the brazilian digital tv system&journal=J Braz Comp Soc&volume=12&issue=4&pages=1-10&publication_year=2007&author=Soares,LFG&author=Rodrigues,RF&author=Moreno,MF)

33.Maas AJ, Nazaré H, Liblit B. Array length inference for c library bindings. In: ASE. New York: ACM: 2016. p. 461–71.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ASE&publication_year=2016&author=Maas,AJ&author=Nazar%C3%A9,H&author=Liblit,B)

34.Fedrecheski G, Costa LCP, Zuffo MK. ISCE. Washington: IEEE: 2016.

35.Rellermeyer JS, Duller M, Gilmer K, Maragkos D, Papageorgiou D, Alonso G. The software fabric for the internet of things. In: IOT. Berlin, Heidelberg: Springer-Verlag: 2008. p. 87–104.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=IOT&publication_year=2008&author=Rellermeyer,JS&author=Duller,M&author=Gilmer,K&author=Maragkos,D&author=Papageorgiou,D&author=Alonso,G)

36.Furr M, Foster JS. Checking type safety of foreign function calls. ACM Trans Program Lang Syst. 2008; 30(4):18:1–18:63.

[Article](https://doi.org/10.1145/1377492.1377493)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Checking type safety of foreign function calls&journal=ACM Trans Program Lang Syst&volume=30&issue=4&pages=18:1-18:63&publication_year=2008&author=Furr,M&author=Foster,JS)

37.Dagenais B, Hendren L. OOPSLA. New York: ACM: 2008. p. 313–28.

38.Melo LTC, Ribeiro RG, de Araújo MR, Pereira FMQ. Inference of static semantics for incomplete c programs. Proc ACM Program Lang. 2017; 2(POPL):29:1–29:28.

[Article](https://doi.org/10.1145/3158117)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Inference of static semantics for incomplete c programs&journal=Proc ACM Program Lang&volume=2&issue=POPL&pages=29:1-29:28&publication_year=2017&author=Melo,LTC&author=Ribeiro,RG&author=de Ara%C3%BAjo,MR&author=Pereira,FMQ)

39.Godefroid P. Micro execution. In: ICSE. New York: ACM: 2014. p. 539–49.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ICSE&publication_year=2014&author=Godefroid,P)

40.Manna Z, Waldinger RJ. Toward automatic program synthesis. Commun ACM. 1971; 14(3):151–65.

[MATH](http://www.emis.de/MATH-item?0214.43006)

[Article](https://doi.org/10.1145/362566.362568)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Toward automatic program synthesis&journal=Commun ACM&volume=14&issue=3&pages=151-65&publication_year=1971&author=Manna,Z&author=Waldinger,RJ)

41.López HA, Marques ERB, Martins F, Ng N, Santos C, Vasconcelos VT, Yoshida N. Protocol-based verification of message-passing parallel programs. In: OOPSLA. New York: ACM: 2015. p. 280–98.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=OOPSLA&publication_year=2015&author=L%C3%B3pez,HA&author=Marques,ERB&author=Martins,F&author=Ng,N&author=Santos,C&author=Vasconcelos,VT&author=Yoshida,N)

42.Bronevetsky G. Communication-sensitive static dataflow for parallel message passing applications. In: CGO. Washington: IEEE: 2009. p. 1–12.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CGO&publication_year=2009&author=Bronevetsky,G)

43.Teixeira FA, Machado GV, Pereira FMQ, Wong HC, Nogueira JMS, Oliveira LB. Siot: Securing the internet of things through distributed system analysis. In: IPSN. New York: ACM: 2015. p. 310–21.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=IPSN&publication_year=2015&author=Teixeira,FA&author=Machado,GV&author=Pereira,FMQ&author=Wong,HC&author=Nogueira,JMS&author=Oliveira,LB)

44.Lhoták O, Hendren L. Context-sensitive points-to analysis: Is it worth it? In: CC. Berlin, Heidelberg: Springer: 2006. p. 47–64.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CC&publication_year=2006&author=Lhot%C3%A1k,O&author=Hendren,L)

45.Agha G. An overview of actor languages. In: OOPWORK. New York: ACM: 1986. p. 58–67.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=OOPWORK&publication_year=1986&author=Agha,G)

46.Haller P, Odersky M. Actors that unify threads and events. In: Proceedings of the 9th International Conference on Coordination Models and Languages. COORDINATION’07. Berlin, Heidelberg: Springer-Verlag: 2007. p. 171–90.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings of the 9th International Conference on Coordination Models and Languages. COORDINATION%E2%80%9907&publication_year=2007&author=Haller,P&author=Odersky,M)

47.Imam SM, Sarkar V. Integrating task parallelism with actors. In: OOPSLA. New York: ACM: 2012. p. 753–72.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=OOPSLA&publication_year=2012&author=Imam,SM&author=Sarkar,V)

48.Cousot P, Cousot R, Logozzo F. A parametric segmentation functor for fully automatic and scalable array content analysis. In: POPL. New York: ACM: 2011. p. 105–18.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=POPL&publication_year=2011&author=Cousot,P&author=Cousot,R&author=Logozzo,F)

49.Nazaré H, Maffra I, Santos W, Barbosa L, Gonnord L, Pereira FMQ. Validation of memory accesses through symbolic analyses. In: OOPSLA. New York: ACM: 2014.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=OOPSLA&publication_year=2014&author=Nazar%C3%A9,H&author=Maffra,I&author=Santos,W&author=Barbosa,L&author=Gonnord,L&author=Pereira,FMQ)

50.Paisante V, Maalej M, Barbosa L, Gonnord L, Pereira FMQ. Symbolic range analysis of pointers. In: CGO. New York: ACM: 2016. p. 171–81.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CGO&publication_year=2016&author=Paisante,V&author=Maalej,M&author=Barbosa,L&author=Gonnord,L&author=Pereira,FMQ)

51.Maalej M, Paisante V, Ramos P, Gonnord L, Pereira FMQ. Pointer disambiguation via strict inequalities. In: Proceedings of the 2017 International Symposium on Code Generation and Optimization, CGO ’17. Piscataway: IEEE Press: 2017. p. 134–47.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings of the 2017 International Symposium on Code Generation and Optimization, CGO %E2%80%9917&publication_year=2017&author=Maalej,M&author=Paisante,V&author=Ramos,P&author=Gonnord,L&author=Pereira,FMQ)

52.Maalej M, Paisante V, Pereira FMQ, Gonnord L. Combining range and inequality information for pointer disambiguation. Sci Comput Program. 2018; 152(C):161–84.

[Article](https://doi.org/10.1016/j.scico.2017.10.014)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Combining range and inequality information for pointer disambiguation&journal=Sci Comput Program&volume=152&issue=C&pages=161-84&publication_year=2018&author=Maalej,M&author=Paisante,V&author=Pereira,FMQ&author=Gonnord,L)

53.Sui Y, Fan X, Zhou H, Xue J. Loop-oriented pointer analysis for automatic simd vectorization. ACM Trans Embed Comput Syst. 2018; 17(2):56:1–56:31.

[Article](https://doi.org/10.1145/3168364)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Loop-oriented pointer analysis for automatic simd vectorization&journal=ACM Trans Embed Comput Syst&volume=17&issue=2&pages=56:1-56:31&publication_year=2018&author=Sui,Y&author=Fan,X&author=Zhou,H&author=Xue,J)

54.Poovendran R. Cyber-physical systems: Close encounters between two parallel worlds [point of view]. Proc IEEE. 2010; 98(8):1363–6.

[Article](https://doi.org/10.1109/JPROC.2010.2050377)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Cyber-physical systems: Close encounters between two parallel worlds [point of view]&journal=Proc IEEE&volume=98&issue=8&pages=1363-6&publication_year=2010&author=Poovendran,R)

55.Conti JP. The internet of things. Commun Eng. 2006; 4(6):20–5.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=2213391)

[Article](https://doi.org/10.1049/ce:20060603)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=The internet of things&journal=Commun Eng&volume=4&issue=6&pages=20-5&publication_year=2006&author=Conti,JP)

56.Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. 2001; 21(6):11–25.

[Article](https://doi.org/10.1109/37.969131)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Identifying, understanding, and analyzing critical infrastructure interdependencies&journal=IEEE Control Syst&volume=21&issue=6&pages=11-25&publication_year=2001&author=Rinaldi,SM&author=Peerenboom,JP&author=Kelly,TK)

57.US Bureau of Transportation Statistics BTS. Average age of automobiles and trucks in operation in the united states. 2017. Accessed 14 Sept 2017.

58.U.S. Department of Transportation. IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments WAVE. 2013.

59.Maurer M, Gerdes JC, Lenz B, Winner H. Autonomous driving: technical, legal and social aspects.Berlin: Springer; 2016.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Autonomous driving: technical, legal and social aspects.&publication_year=2016&author=Maurer,M&author=Gerdes,JC&author=Lenz,B&author=Winner,H)

60.Patel N. 90% of startups fail: Here is what you need to know about the 10%. 2015. <https://www.forbes.com/sites/neilpatel/2015/01/16/90-of-startups-will-fail-heres-what-you-need-to-know-about-the-10/>. Accessed 09 Sept 2018.

61.Jacobsson A, Boldt M, Carlsson B. A risk analysis of a smart home automation system. Futur Gener Comput Syst. 2016; 56(Supplement C):719–33.

[Article](https://doi.org/10.1016/j.future.2015.09.003)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A risk analysis of a smart home automation system&journal=Futur Gener Comput Syst&volume=56&issue=Supplement C&pages=719-33&publication_year=2016&author=Jacobsson,A&author=Boldt,M&author=Carlsson,B)

62.Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978; 21(2):120–6.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=700103)

[MATH](http://www.emis.de/MATH-item?0368.94005)

[Article](https://doi.org/10.1145/359340.359342)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A method for obtaining digital signatures and public-key cryptosystems&journal=Commun ACM&volume=21&issue=2&pages=120-6&publication_year=1978&author=Rivest,RL&author=Shamir,A&author=Adleman,LM)

63.Miller VS. Use of elliptic curves in cryptography. In: CRYPTO, volume 218 of Lecture Notes in Computer Science. Berlin: Springer: 1985. p. 417–26.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CRYPTO, volume 218 of Lecture Notes in Computer Science&publication_year=1985&author=Miller,VS)

64.Koblitz N. Elliptic curve cryptosystems. Math Comput. 1987; 48(177):203–9.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=866109)

[MATH](http://www.emis.de/MATH-item?0622.94015)

[Article](https://doi.org/10.1090/S0025-5718-1987-0866109-5)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Elliptic curve cryptosystems&journal=Math Comput&volume=48&issue=177&pages=203-9&publication_year=1987&author=Koblitz,N)

65.Barbulescu R, Gaudry P, Joux A, Thomé E. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: EUROCRYPT 2014. Berlin: Springer: 2014. p. 1–16.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=EUROCRYPT 2014&publication_year=2014&author=Barbulescu,R&author=Gaudry,P&author=Joux,A&author=Thom%C3%A9,E)

66.Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theor. 2006; 22(6):644–54.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=437208)

[MATH](http://www.emis.de/MATH-item?0435.94018)

[Article](https://doi.org/10.1109/TIT.1976.1055638)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=New directions in cryptography&journal=IEEE Trans Inf Theor&volume=22&issue=6&pages=644-54&publication_year=2006&author=Diffie,W&author=Hellman,M)

67.Barker E. Federal Information Processing Standards Publication (FIPS PUB) 186-4 Digital Signature Standard (DSS). 2013.

68.Barker E, Johnson D, Smid M. Special publication 800-56A recommendation for pair-wise key establishment schemes using discrete logarithm cryptography. 2006.

69.Simon DR. On the power of quantum computation. In: Symposium on Foundations of Computer Science (SFCS 94). Washington: IEEE Computer Society: 1994. p. 116–23.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Symposium on Foundations of Computer Science (SFCS 94)&publication_year=1994&author=Simon,DR)

70.Knill E. Physics: quantum computing. Nature. 2010; 463(7280):441–3.

[Article](https://doi.org/10.1038/463441a)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Physics: quantum computing&journal=Nature&volume=463&issue=7280&pages=441-3&publication_year=2010&author=Knill,E)

71.Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of ACM STOC 1996. New York: ACM: 1996. p. 212–19.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings of ACM STOC 1996&publication_year=1996&author=Grover,LK)

72.Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput. 1997; 26(5):1484–509.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=1471990)

[MATH](http://www.emis.de/MATH-item?1005.11065)

[Article](https://doi.org/10.1137/S0097539795293172)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer&journal=SIAM J Comput&volume=26&issue=5&pages=1484-509&publication_year=1997&author=Shor,PW)

73.McEliece RJ. A public-key cryptosystem based on algebraic coding theory. Deep Space Netw. 1978; 44:114–6.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A public-key cryptosystem based on algebraic coding theory&journal=Deep Space Netw&volume=44&pages=114-6&publication_year=1978&author=McEliece,RJ)

74.Merkle RC. Secrecy, authentication and public key systems / A certified digital signature. PhD thesis, Stanford. 1979.

75.Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of ACM STOC ’05. STOC ’05. New York: ACM: 2005. p. 84–93.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings of ACM STOC %E2%80%9905. STOC %E2%80%9905&publication_year=2005&author=Regev,O)

76.Buchmann J, Dahmen E, Hülsing A. Xmss - a practical forward secure signature scheme based on minimal security assumptions In: Yang B-Y, editor. PQCrypto. Berlin: Springer: 2011. p. 117–29.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=PQCrypto&publication_year=2011&author=Buchmann,J&author=Dahmen,E&author=H%C3%BClsing,A)

77.McGrew DA, Curcio M, Fluhrer S. Hash-Based Signatures. Internet Engineering Task Force (IETF). 2017. <https://datatracker.ietf.org/doc/html/draft-mcgrew-hash-sigs-13>. Accessed 9 Sept 2018.

78.Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE ICCSSP’84. New York: IEEE Press: 1984. p. 175–9.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings of IEEE ICCSSP%E2%80%9984&publication_year=1984&author=Bennett,CH&author=Brassard,G)

79.Bos J, Costello C, Ducas L, Mironov I, Naehrig M, Nikolaenko V, Raghunathan A, Stebila D. Frodo: Take off the ring! practical, quantum-secure key exchange from LWE. Cryptology ePrint Archive, Report 2016/659. 2016. <http://eprint.iacr.org/2016/659>.

80.Alkim E, Ducas L, Pöppelmann T, Schwabe P. Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Report 2015/1092. 2015. <http://eprint.iacr.org/2015/1092>.

81.Misoczki R, Tillich J-P, Sendrier N, PBarreto LSM. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In: IEEE International Symposium on Information Theory – ISIT’2013. Istambul: IEEE: 2013. p. 2069–73.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=IEEE International Symposium on Information Theory %E2%80%93 ISIT%E2%80%992013&publication_year=2013&author=Misoczki,R&author=Tillich,J-P&author=Sendrier,N&author=PBarreto,LSM)

82.Hoffstein J, Pipher J, Silverman JH. Ntru: A ring-based public key cryptosystem. In: International Algorithmic Number Theory Symposium. Berlin: Springer: 1998. p. 267–88.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=International Algorithmic Number Theory Symposium&publication_year=1998&author=Hoffstein,J&author=Pipher,J&author=Silverman,JH)

83.Bos J, Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schanck JM, Schwabe P, Stehlé D. Crystals–kyber: a CCA-secure module-lattice-based KEM. IACR Cryptol ePrint Arch. 2017; 2017:634.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Crystals%E2%80%93kyber: a CCA-secure module-lattice-based KEM&journal=IACR Cryptol ePrint Arch&volume=2017&publication_year=2017&author=Bos,J&author=Ducas,L&author=Kiltz,E&author=Lepoint,T&author=Lyubashevsky,V&author=Schanck,JM&author=Schwabe,P&author=Stehl%C3%A9,D)

84.Aragon N, Barreto PSLM, Bettaieb S, Bidoux L, Blazy O, Deneuville J-C, Gaborit P, Gueron S, Guneysu T, Melchor CA, Misoczki R, Persichetti E, Sendrier N, Tillich J-P, Zemor G. BIKE: Bit flipping key encapsulation. Submission to the NIST Standardization Process on Post-Quantum Cryptography. 2017. <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions>.

85.Barreto PSLM, Gueron S, Gueneysu T, Misoczki R, Persichetti E, Sendrier N, Tillich J-P. Cake: Code-based algorithm for key encapsulation. In: IMA International Conference on Cryptography and Coding. Berlin: Springer: 2017. p. 207–26.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=IMA International Conference on Cryptography and Coding&publication_year=2017&author=Barreto,PSLM&author=Gueron,S&author=Gueneysu,T&author=Misoczki,R&author=Persichetti,E&author=Sendrier,N&author=Tillich,J-P)

86.Jao D, De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: International Workshop on Post-Quantum Cryptography. Berlin: Springer: 2011. p. 19–34.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=International Workshop on Post-Quantum Cryptography&publication_year=2011&author=Jao,D&author=De Feo,L)

87.Costello C, Jao D, Longa P, Naehrig M, Renes J, Urbanik D. Efficient compression of sidh public keys. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer: 2017. p. 679–706.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Annual International Conference on the Theory and Applications of Cryptographic Techniques&publication_year=2017&author=Costello,C&author=Jao,D&author=Longa,P&author=Naehrig,M&author=Renes,J&author=Urbanik,D)

88.Jao D, Azarderakhsh R, Campagna M, Costello C, DeFeo L, Hess B, Jalali A, Koziel B, LaMacchia B, Longa P, Naehrig M, Renes J, Soukharev V, Urbanik D. SIKE: Supersingular isogeny key encapsulation. Submission to the NIST Standardization Process on Post-Quantum Cryptography. 2017. <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions>.

89.Galbraith SD, Petit C, Shani B, Ti YB. On the security of supersingular isogeny cryptosystems. In: International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer: 2016. p. 63–91.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=International Conference on the Theory and Application of Cryptology and Information Security&publication_year=2016&author=Galbraith,SD&author=Petit,C&author=Shani,B&author=Ti,YB)

90.National Institute of Standards and Technology (NIST). Standardization Process on Post-Quantum Cryptography. 2016. <http://csrc.nist.gov/groups/ST/post-quantum-crypto/>. Accessed 9 Sept 2018.

91.McGrew D, Kampanakis P, Fluhrer S, Gazdag S-L, Butin D, Buchmann J. State management for hash-based signatures. In: International Conference on Research in Security Standardization. Springer: 2016. p. 244–60.

92.Bernstein DJ, Hopwood D, Hülsing A, Lange T, Niederhagen R, Papachristodoulou L, Schneider M, Schwabe P, Wilcox-O’Hearn Z. SPHINCS: Practical Stateless Hash-Based Signatures. Berlin, Heidelberg: Springer Berlin Heidelberg; 2015. p. 368–97.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=SPHINCS: Practical Stateless Hash-Based Signatures&publication_year=2015&author=Bernstein,DJ&author=Hopwood,D&author=H%C3%BClsing,A&author=Lange,T&author=Niederhagen,R&author=Papachristodoulou,L&author=Schneider,M&author=Schwabe,P&author=Wilcox-O%E2%80%99Hearn,Z)

93.Barker E, Barker W, Burr W, Polk W, Smid M. Recommendation for key management part 1: General (revision 3). NIST Spec Publ. 2012; 800(57):1–147.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Recommendation for key management part 1: General (revision 3)&journal=NIST Spec Publ&volume=800&issue=57&pages=1-147&publication_year=2012&author=Barker,E&author=Barker,W&author=Burr,W&author=Polk,W&author=Smid,M)

94.Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Public Key Cryptography. LNCS, 6571 vol.Berlin: Springer: 2011. p. 53–70.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Public Key Cryptography. LNCS, 6571 vol.&publication_year=2011&author=Waters,B)

95.Liu Z, Wong DS. Practical attribute-based encryption: Traitor tracing, revocation and large universe. Comput J. 2016; 59(7):983–1004.

[Article](https://doi.org/10.1093/comjnl/bxv101)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Practical attribute-based encryption: Traitor tracing, revocation and large universe&journal=Comput J&volume=59&issue=7&pages=983-1004&publication_year=2016&author=Liu,Z&author=Wong,DS)

96.Oliveira LB, Aranha DF, Gouvêa CPL, Scott M, Câmara DF, López J, Dahab R. Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Comput Commun. 2011; 34(3):485–93.

[Article](https://doi.org/10.1016/j.comcom.2010.05.013)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks&journal=Comput Commun&volume=34&issue=3&pages=485-93&publication_year=2011&author=Oliveira,LB&author=Aranha,DF&author=Gouv%C3%AAa,CPL&author=Scott,M&author=C%C3%A2mara,DF&author=L%C3%B3pez,J&author=Dahab,R)

97.Kim T, Barbulescu R. Extended tower number field sieve: A new complexity for the medium prime case. In: CRYPTO (1). LNCS, 9814 vol.Berlin: Springer: 2016. p. 543–71.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CRYPTO (1). LNCS, 9814 vol.&publication_year=2016&author=Kim,T&author=Barbulescu,R)

98.Boneh D, Franklin MK. Identity-based encryption from the weil pairing. SIAM J Comput. 2003; 32(3):586–615.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=2001745)

[MATH](http://www.emis.de/MATH-item?1046.94008)

[Article](https://doi.org/10.1137/S0097539701398521)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Identity-based encryption from the weil pairing&journal=SIAM J Comput&volume=32&issue=3&pages=586-615&publication_year=2003&author=Boneh,D&author=Franklin,MK)

99.Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: ASIACRYPT. LNCS, 2894 vol.Berlin: Springer: 2003. p. 452–73.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ASIACRYPT. LNCS, 2894 vol.&publication_year=2003&author=Al-Riyami,SS&author=Paterson,KG)

100.Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation. IACR Cryptol ePrint Arch. 2012; 2012:52.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Identity-based encryption with efficient revocation&journal=IACR Cryptol ePrint Arch&volume=2012&publication_year=2012&author=Boldyreva,A&author=Goyal,V&author=Kumar,V)

101.Simplício Jr. MA, Silva MVM, Alves RCA, Shibata TKC. Lightweight and escrow-less authenticated key agreement for the internet of things. Comput Commun. 2017; 98:43–51.

[Article](https://doi.org/10.1016/j.comcom.2016.05.002)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Lightweight and escrow-less authenticated key agreement for the internet of things&journal=Comput Commun&volume=98&pages=43-51&publication_year=2017&author=Simpl%C3%ADcio Jr.,MA&author=Silva,MVM&author=Alves,RCA&author=Shibata,TKC)

102.Neto ALM, Souza ALF, Cunha ÍS, Nogueira M, Nunes IO, Cotta L, Gentille N, Loureiro AAF, Aranha DF, Patil HK, Oliveira LB. Aot: Authentication and access control for the entire iot device life-cycle. In: SenSys. New York: ACM: 2016. p. 1–15.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=SenSys&publication_year=2016&author=Neto,ALM&author=Souza,ALF&author=Cunha,%C3%8DS&author=Nogueira,M&author=Nunes,IO&author=Cotta,L&author=Gentille,N&author=Loureiro,AAF&author=Aranha,DF&author=Patil,HK&author=Oliveira,LB)

103.Mouha N. The design space of lightweight cryptography. IACR Cryptol ePrint Arch. 2015; 2015:303.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=The design space of lightweight cryptography&journal=IACR Cryptol ePrint Arch&volume=2015&publication_year=2015&author=Mouha,N)

104.Daemen J, Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Berlin: Springer; 2002.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography&publication_year=2002&author=Daemen,J&author=Rijmen,V)

105.Grosso V, Leurent G, Standaert F-X, Varici K. Ls-designs: Bitslice encryption for efficient masked software implementations. In: FSE. LNCS, 8540 vol.Berlin: Springer: 2014. p. 18–37.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=FSE. LNCS, 8540 vol.&publication_year=2014&author=Grosso,V&author=Leurent,G&author=Standaert,F-X&author=Varici,K)

106.Dinu D, Perrin L, Udovenko A, Velichkov V, Großschädl J, Biryukov A. Design strategies for ARX with provable bounds: Sparx and LAX. In: ASIACRYPT (1). LNCS, 10031 vol.Berlin: Springer: 2016. p. 484–513.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ASIACRYPT (1). LNCS, 10031 vol.&publication_year=2016&author=Dinu,D&author=Perrin,L&author=Udovenko,A&author=Velichkov,V&author=Gro%C3%9Fsch%C3%A4dl,J&author=Biryukov,A)

107.Albrecht MR, Driessen B, Kavun EB, Leander G, Paar C, Yalçin T. Block ciphers - focus on the linear layer (feat. PRIDE). In: CRYPTO (1). LNCS, 8616 vol.Berlin: Springer: 2014. p. 57–76.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CRYPTO (1). LNCS, 8616 vol.&publication_year=2014&author=Albrecht,MR&author=Driessen,B&author=Kavun,EB&author=Leander,G&author=Paar,C&author=Yal%C3%A7in,T)

108.Beierle C, Jean J, Kölbl S, Leander G, Moradi A, Peyrin T, Sasaki Y, Sasdrich P, Sim SM. The SKINNY family of block ciphers and its low-latency variant MANTIS. In: CRYPTO (2). LNCS, 9815 vol.Berlin: Springer: 2016. p. 123–53.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CRYPTO (2). LNCS, 9815 vol.&publication_year=2016&author=Beierle,C&author=Jean,J&author=K%C3%B6lbl,S&author=Leander,G&author=Moradi,A&author=Peyrin,T&author=Sasaki,Y&author=Sasdrich,P&author=Sim,SM)

109.Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJB, Seurin Y, Vikkelsoe C. PRESENT: an ultra-lightweight block cipher. In: CHES. LNCS, 4727 vol.Berlin: Springer: 2007. p. 450–66.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CHES. LNCS, 4727 vol.&publication_year=2007&author=Bogdanov,A&author=Knudsen,LR&author=Leander,G&author=Paar,C&author=Poschmann,A&author=Robshaw,MJB&author=Seurin,Y&author=Vikkelsoe,C)

110.Reis TBS, Aranha DF, López J. PRESENT runs fast - efficient and secure implementation in software. In: CHES, volume 10529 of Lecture Notes in Computer Science. Berlin: Springer: 2017. p. 644–64.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CHES, volume 10529 of Lecture Notes in Computer Science&publication_year=2017&author=Reis,TBS&author=Aranha,DF&author=L%C3%B3pez,J)

111.Aumasson J-P, Bernstein DJ. Siphash: A fast short-input PRF. In: INDOCRYPT. LNCS, 7668 vol.Berlin: Springer: 2012. p. 489–508.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=INDOCRYPT. LNCS, 7668 vol.&publication_year=2012&author=Aumasson,J-P&author=Bernstein,DJ)

112.Kölbl S, Lauridsen MM, Mendel F, Rechberger C. Haraka v2 - efficient short-input hashing for post-quantum applications. IACR Trans Symmetric Cryptol. 2016; 2016(2):1–29.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Haraka v2 - efficient short-input hashing for post-quantum applications&journal=IACR Trans Symmetric Cryptol&volume=2016&issue=2&pages=1-29&publication_year=2016&author=K%C3%B6lbl,S&author=Lauridsen,MM&author=Mendel,F&author=Rechberger,C)

113.Aumasson J-P, Neves S, Wilcox-O’Hearn Z, Winnerlein C. BLAKE2: simpler, smaller, fast as MD5. In: ACNS. LNCS, 7954 vol.Berlin: Springer: 2013. p. 119–35.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ACNS. LNCS, 7954 vol.&publication_year=2013&author=Aumasson,J-P&author=Neves,S&author=Wilcox-O%E2%80%99Hearn,Z&author=Winnerlein,C)

114.Stevens M, Karpman P, Peyrin T. Freestart collision for full SHA-1. In: EUROCRYPT (1). LNCS, 9665 vol.Berlin: Springer: 2016. p. 459–83.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=EUROCRYPT (1). LNCS, 9665 vol.&publication_year=2016&author=Stevens,M&author=Karpman,P&author=Peyrin,T)

115.NIST Computer Security Division. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. FIPS Publication 202, National Institute of Standards and Technology, U.S. Department of Commerce, May 2014.

116.McGrew DA, Viega J. The security and performance of the galois/counter mode (GCM) of operation. In: INDOCRYPT. LNCS, 3348 vol.Berlin: Springer: 2004. p. 343–55.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=INDOCRYPT. LNCS, 3348 vol.&publication_year=2004&author=McGrew,DA&author=Viega,J)

117.Koblitz N. A family of jacobians suitable for discrete log cryptosystems. In: CRYPTO, volume 403 of LNCS. Berlin: Springer: 1988. p. 94–99.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CRYPTO, volume 403 of LNCS&publication_year=1988&author=Koblitz,N)

118.Bernstein DJ. Curve25519: New diffie-hellman speed records. In: Public Key Cryptography. LNCS, 3958 vol.Berlin: Springer: 2006. p. 207–28.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Public Key Cryptography. LNCS, 3958 vol.&publication_year=2006&author=Bernstein,DJ)

119.Bernstein DJ, Duif N, Lange T, Schwabe P, Yang B-Y. High-speed high-security signatures. J Cryptographic Eng. 2012; 2(2):77–89.

[MATH](http://www.emis.de/MATH-item?1321.94039)

[Article](https://doi.org/10.1007/s13389-012-0027-1)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=High-speed high-security signatures&journal=J Cryptographic Eng&volume=2&issue=2&pages=77-89&publication_year=2012&author=Bernstein,DJ&author=Duif,N&author=Lange,T&author=Schwabe,P&author=Yang,B-Y)

120.Costello C, Longa P. FourQQ : Four-dimensional decompositions on a QQ -curve over the mersenne prime. In: ASIACRYPT (1). LNCS, 9452 vol.Berlin: Springer: 2015. p. 214–35.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ASIACRYPT (1). LNCS, 9452 vol.&publication_year=2015&author=Costello,C&author=Longa,P)

121.Banik S, Bogdanov A, Regazzoni F. Exploring energy efficiency of lightweight block ciphers. In: SAC. LNCS, 9566 vol.Berlin: Springer: 2015. p. 178–94.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=SAC. LNCS, 9566 vol.&publication_year=2015&author=Banik,S&author=Bogdanov,A&author=Regazzoni,F)

122.Dinu D, Corre YL, Khovratovich D, Perrin L, Großschädl J, Biryukov A. Triathlon of lightweight block ciphers for the internet of things. NIST Workshop on Lightweight Cryptography. 2015.

123.Kocher PC. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In: CRYPTO. LNCS, 1109 vol.Berlin: Springer: 1996. p. 104–13.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CRYPTO. LNCS, 1109 vol.&publication_year=1996&author=Kocher,PC)

124.Rodrigues B, Pereira FMQ, Aranha DF. Sparse representation of implicit flows with applications to side-channel detection In: Zaks A, Hermenegildo MV, editors. Proceedings of the 25th International Conference on Compiler Construction, CC 2016, Barcelona, Spain, March 12-18, 2016. New York: ACM: 2016. p. 110–20.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings of the 25th International Conference on Compiler Construction, CC 2016, Barcelona, Spain, March 12-18, 2016&publication_year=2016&author=Rodrigues,B&author=Pereira,FMQ&author=Aranha,DF)

125.Almeida JB, Barbosa M, Barthe G, Dupressoir F, Emmi M. Verifying constant-time implementations. In: USENIX Security Symposium. Berkeley: USENIX Association: 2016. p. 53–70.

126.Kocher PC, Jaffe J, Jun B. Differential power analysis. In: CRYPTO. LNCS, 1666 vol. Springer: 1999. p. 388–97.

127.Biham E, Shamir A. Differential fault analysis of secret key cryptosystems. In: CRYPTO. LNCS, 1294 vol.Berlin: Springer: 1997. p. 513–25.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CRYPTO. LNCS, 1294 vol.&publication_year=1997&author=Biham,E&author=Shamir,A)

128.Kim Y, Daly R, Kim J, Fallin C, Lee J-H, Lee D, Wilkerson C, Lai K, Mutlu O. Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. In: ISCA. Washington, DC: IEEE Computer Society: 2014. p. 361–72.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ISCA&publication_year=2014&author=Kim,Y&author=Daly,R&author=Kim,J&author=Fallin,C&author=Lee,J-H&author=Lee,D&author=Wilkerson,C&author=Lai,K&author=Mutlu,O)

129.Ishai Y, Sahai A, Wagner D. Private circuits: Securing hardware against probing attacks. In: CRYPTO. LNCS, 2729 vol. Springer: 2003. p. 463–81.

130.Balasch J, Gierlichs B, Grosso V, Reparaz O, Standaert F-X. On the cost of lazy engineering for masked software implementations. In: CARDIS. LNCS, 8968 vol.Berlin: Springer: 2014. p. 64–81.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=CARDIS. LNCS, 8968 vol.&publication_year=2014&author=Balasch,J&author=Gierlichs,B&author=Grosso,V&author=Reparaz,O&author=Standaert,F-X)

131.Nogueira M, dos Santos AL, Pujolle G. A survey of survivability in mobile ad hoc networks. IEEE Commun Surv Tutor. 2009; 11(1):66–77.

[Article](https://doi.org/10.1109/SURV.2009.090106)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A survey of survivability in mobile ad hoc networks&journal=IEEE Commun Surv Tutor&volume=11&issue=1&pages=66-77&publication_year=2009&author=Nogueira,M&author=dos Santos,AL&author=Pujolle,G)

132.Mansfield-Devine S. The growth and evolution of ddos. Netw Secur. 2015; 2015(10):13–20.

[Article](https://doi.org/10.1016/S1353-4858(15)30092-1)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=The growth and evolution of ddos&journal=Netw Secur&volume=2015&issue=10&pages=13-20&publication_year=2015&author=Mansfield-Devine,S)

133.Thielman S, Johnston C. Major Cyber Attack Disrupts Internet Service Across Europe and US. <https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service>. Accessed 3 July 2018.

134.DDoS attacks: For the hell of it or targeted – how do you see them off?<http://www.theregister.co.uk/2016/09/22/ddos_attack_defence/>. Accessed 14 Feb 2017.

135.Santos AA, Nogueira M, Moura JMF. A stochastic adaptive model to explore mobile botnet dynamics. IEEE Commun Lett. 2017; 21(4):753–6.

[Article](https://doi.org/10.1109/LCOMM.2016.2637367)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A stochastic adaptive model to explore mobile botnet dynamics&journal=IEEE Commun Lett&volume=21&issue=4&pages=753-6&publication_year=2017&author=Santos,AA&author=Nogueira,M&author=Moura,JMF)

136.Macedo R, de Castro R, Santos A, Ghamri-Doudane Y, Nogueira M. Self-organized SDN controller cluster conformations against DDoS attacks effects. In: 2016 IEEE Global Communications Conference, GLOBECOM, 2016, Washington, DC, USA, December 4–8, 2016. Piscataway: IEEE: 2016. p. 1–6.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=2016 IEEE Global Communications Conference, GLOBECOM, 2016, Washington, DC, USA, December 4%E2%80%938, 2016&publication_year=2016&author=Macedo,R&author=de Castro,R&author=Santos,A&author=Ghamri-Doudane,Y&author=Nogueira,M)

137.Soto J, Nogueira M. A framework for resilient and secure spectrum sensing on cognitive radio networks. Comput Netw. 2015; 79:313–22.

[Article](https://doi.org/10.1016/j.comnet.2015.01.011)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A framework for resilient and secure spectrum sensing on cognitive radio networks&journal=Comput Netw&volume=79&pages=313-22&publication_year=2015&author=Soto,J&author=Nogueira,M)

138.Lipa N, Mannes E, Santos A, Nogueira M. Firefly-inspired and robust time synchronization for cognitive radio ad hoc networks. Comput Commun. 2015; 66:36–44.

[Article](https://doi.org/10.1016/j.comcom.2015.04.005)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Firefly-inspired and robust time synchronization for cognitive radio ad hoc networks&journal=Comput Commun&volume=66&pages=36-44&publication_year=2015&author=Lipa,N&author=Mannes,E&author=Santos,A&author=Nogueira,M)

139.Zhang C, Song Y, Fang Y. Modeling secure connectivity of self-organized wireless ad hoc networks. In: IEEE INFOCOM. Piscataway: IEEE: 2008. p. 251–5.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=IEEE INFOCOM&publication_year=2008&author=Zhang,C&author=Song,Y&author=Fang,Y)

140.Salem NB, Hubaux J-P. Securing wireless mesh networks. IEEE Wirel Commun. 2006; 13(2):50–5.

[Article](https://doi.org/10.1109/MWC.2006.1632480)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Securing wireless mesh networks&journal=IEEE Wirel Commun&volume=13&issue=2&pages=50-5&publication_year=2006&author=Salem,NB&author=Hubaux,J-P)

141.Yang H, Luo H, Ye F, Lu S, Zhang L. Security in mobile ad hoc networks: challenges and solutions. IEEE Wirel Commun. 2004; 11(1):38–47.

[Article](https://doi.org/10.1109/MWC.2004.1269716)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Security in mobile ad hoc networks: challenges and solutions&journal=IEEE Wirel Commun&volume=11&issue=1&pages=38-47&publication_year=2004&author=Yang,H&author=Luo,H&author=Ye,F&author=Lu,S&author=Zhang,L)

142.Nogueira M. SAMNAR: A survivable architecture for wireless self-organizing networks. PhD thesis, Université Pierre et Marie Curie - LIP6. 2009.

143.ITU. NGN identity management framework: International Telecommunication Union (ITU); 2009. Recommendation Y.2720.

144.Lopez J, Oppliger R, Pernul G. Authentication and authorization infrastructures (aais): a comparative survey. Comput Secur. 2004; 23(7):578–90.

[Article](https://doi.org/10.1016/j.cose.2004.06.013)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Authentication and authorization infrastructures (aais): a comparative survey&journal=Comput Secur&volume=23&issue=7&pages=578-90&publication_year=2004&author=Lopez,J&author=Oppliger,R&author=Pernul,G)

145.Arias-Cabarcos P, Almenárez F, Trapero R, Díaz-Sánchez D, Marín A. Blended identity: Pervasive idm for continuous authentication. IEEE Secur Priv. 2015; 13(3):32–39.

[Article](https://doi.org/10.1109/MSP.2015.62)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Blended identity: Pervasive idm for continuous authentication&journal=IEEE Secur Priv&volume=13&issue=3&pages=32-39&publication_year=2015&author=Arias-Cabarcos,P&author=Almen%C3%A1rez,F&author=Trapero,R&author=D%C3%ADaz-S%C3%A1nchez,D&author=Mar%C3%ADn,A)

146.Bhargav-Spantzel A, Camenisch J, Gross T, Sommer D. User centricity: a taxonomy and open issues. J Comput Secur. 2007; 15(5):493–527.

[Article](https://doi.org/10.3233/JCS-2007-15502)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=User centricity: a taxonomy and open issues&journal=J Comput Secur&volume=15&issue=5&pages=493-527&publication_year=2007&author=Bhargav-Spantzel,A&author=Camenisch,J&author=Gross,T&author=Sommer,D)

147.Garcia-Morchon O, Kumar S, Sethi M, Internet Engineering Task Force. State-of-the-art and challenges for the internet of things security. Internet Engineering Task Force; 2017. <https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-iot-seccons-04>.

148.Torres J, Nogueira M, Pujolle G. A survey on identity management for the future network. IEEE Commun Surv Tutor. 2013; 15(2):787–802.

[Article](https://doi.org/10.1109/SURV.2012.072412.00129)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A survey on identity management for the future network&journal=IEEE Commun Surv Tutor&volume=15&issue=2&pages=787-802&publication_year=2013&author=Torres,J&author=Nogueira,M&author=Pujolle,G)

149.Hanumanthappa P, Singh S. Privacy preserving and ownership authentication in ubiquitous computing devices using secure three way authentication. In: Proceedings. International Conference on Innovations in Information Technology (IIT): 2012. p. 107–12.

150.Fremantle P, Aziz B, Kopecký J, Scott P. Federated identity and access management for the internet of things. In: 2014 International Workshop on Secure Internet of Things: 2014. p. 10–17.

151.Domenech MC, Boukerche A, Wangham MS. An authentication and authorization infrastructure for the web of things. In: Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Q2SWinet ’16. New York: ACM: 2016. p. 39–46.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Q2SWinet %E2%80%9916&publication_year=2016&author=Domenech,MC&author=Boukerche,A&author=Wangham,MS)

152.Birrell E, Schneider FB. Federated identity management systems: A privacy-based characterization. IEEE Secur Priv. 2013; 11(5):36–48.

[Article](https://doi.org/10.1109/MSP.2013.114)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Federated identity management systems: A privacy-based characterization&journal=IEEE Secur Priv&volume=11&issue=5&pages=36-48&publication_year=2013&author=Birrell,E&author=Schneider,FB)

153.Nguyen T-D, Al-Saffar A, Huh E-N. A dynamic id-based authentication scheme. In: Proceedings. Sixth International Conference on Networked Computing and Advanced Information Management (NCM), 2010.2010. p. 248–53.

154.Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the internet of things. Math Comput Model. 2013; 58:1189–205.

[Article](https://doi.org/10.1016/j.mcm.2013.02.006)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A capability-based security approach to manage access control in the internet of things&journal=Math Comput Model&volume=58&pages=1189-205&publication_year=2013&author=Gusmeroli,S&author=Piccione,S&author=Rotondi,D)

155.Akram H, Hoffmann M. Supports for identity management in ambient environments-the hydra approach. In: Proceedings. 3rd International Conference on Systems and Networks Communications, 2008. ICSNC’08.2008. p. 371–7.

156.Liu J, Xiao Y, Chen CLP. Authentication and access control in the internet of things. In: Proceedings. 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW) 2012.2012. p. 588–92.

157.Ndibanje B, Lee H-J, Lee S-G. Security analysis and improvements of authentication and access control in the internet of things. Sensors. 2014; 14(8):14786–805.

[Article](https://doi.org/10.3390/s140814786)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Security analysis and improvements of authentication and access control in the internet of things&journal=Sensors&volume=14&issue=8&pages=14786-805&publication_year=2014&author=Ndibanje,B&author=Lee,H-J&author=Lee,S-G)

158.Kim Y-P, Yoo S, Yoo C. Daot: Dynamic and energy-aware authentication for smart home appliances in internet of things. In: Consumer Electronics (ICCE), 2015 IEEE International Conference on.2015. p. 196–7.

159.Markmann T, Schmidt TC, Wählisch M. Federated end-to-end authentication for the constrained internet of things using ibc and ecc. SIGCOMM Comput Commun Rev. 2015; 45(4):603–4.

[Article](https://doi.org/10.1145/2829988.2790021)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Federated end-to-end authentication for the constrained internet of things using ibc and ecc&journal=SIGCOMM Comput Commun Rev&volume=45&issue=4&pages=603-4&publication_year=2015&author=Markmann,T&author=Schmidt,TC&author=W%C3%A4hlisch,M)

160.Dasgupta D, Roy A, Nag A. Multi-factor authentication. Cham: Springer International Publishing; 2017. p. 185–233.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Multi-factor authentication&publication_year=2017&author=Dasgupta,D&author=Roy,A&author=Nag,A)

161.NIST. Digital Identity Guidelines. NIST Special Publication 800-63-3. 2017. <https://doi.org/10.6028/NIST.SP.800-63-3>.

162.Dzurenda P, Hajny J, Zeman V, Vrba K. Modern physical access control systems and privacy protection. In: 2015 38th International Conference on Telecommunications and Signal Processing (TSP).2015. p. 1–5.

163.Guinard D, Fischer M, Trifa V. Sharing using social networks in a composable web of things. In: Proceedings. 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010.2010. p. 702–7.

164.Rotondi D, Seccia C, Piccione S. Access control & IoT: Capability based authorization access control system. In: Proceedings. 1st IoT International Forum: 2011.

165.Mahalle PN, Anggorojati B, Prasad NR, Prasad R. Identity authentication and capability based access control (iacac) for the internet of things. J Cyber Secur Mob. 2013; 1(4):309–48.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Identity authentication and capability based access control (iacac) for the internet of things&journal=J Cyber Secur Mob&volume=1&issue=4&pages=309-48&publication_year=2013&author=Mahalle,PN&author=Anggorojati,B&author=Prasad,NR&author=Prasad,R)

166.Moreira Sá De Souza L, Spiess P, Guinard D, Köhler M, Karnouskos S, Savio D. Socrades: A web service based shop floor integration infrastructure. In: The internet of things. Springer: 2008. p. 50–67.

167.Jindou J, Xiaofeng Q, Cheng C. Access control method for web of things based on role and sns. In: Proceedings. IEEE 12th International Conference on Computer and Information Technology (CIT), 2012. Washington: IEEE Computer Society: 2012. p. 316–21.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings. IEEE 12th International Conference on Computer and Information Technology (CIT), 2012&publication_year=2012&author=Jindou,J&author=Xiaofeng,Q&author=Cheng,C)

168.Han Q, Li J. An authorization management approach in the internet of things. J Inf Comput Sci. 2012; 9(6):1705–13.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=An authorization management approach in the internet of things&journal=J Inf Comput Sci&volume=9&issue=6&pages=1705-13&publication_year=2012&author=Han,Q&author=Li,J)

169.Zhang G, Liu J. A model of workflow-oriented attributed based access control. Int J Comput Netw Inf Secur (IJCNIS). 2011; 3(1):47–53.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A model of workflow-oriented attributed based access control&journal=Int J Comput Netw Inf Secur (IJCNIS)&volume=3&issue=1&pages=47-53&publication_year=2011&author=Zhang,G&author=Liu,J)

170.do Prado Filho TG, Vinicius Serafim Prazeres C. Multiauth-wot: A multimodal service for web of things athentication and identification. In: Proceedings of the 21st Brazilian Symposium on Multimedia and the Web, WebMedia ’15. New York: ACM: 2015. p. 17–24.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings of the 21st Brazilian Symposium on Multimedia and the Web, WebMedia %E2%80%9915&publication_year=2015&author=do Prado Filho,TG&author=Vinicius Serafim Prazeres,C)

171.Alam S, Chowdhury MMR, Noll J. Interoperability of security-enabled internet of things. Wirel Pers Commun. 2011; 61(3):567–86.

[Article](https://doi.org/10.1007/s11277-011-0384-6)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Interoperability of security-enabled internet of things&journal=Wirel Pers Commun&volume=61&issue=3&pages=567-86&publication_year=2011&author=Alam,S&author=Chowdhury,MMR&author=Noll,J)

172.Seitz L, Selander G, Gehrmann C. Authorization framework for the internet-of-things. In: Proceedings. IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). Washington, DC: IEEE Computer Society: 2013. p. 1–6.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings. IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)&publication_year=2013&author=Seitz,L&author=Selander,G&author=Gehrmann,C)

173.OASIS. Saml v2.0 executive overview. 2005. <https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf>.

174.Hardt D. The oauth 2.0 authorization framework. RFC 6749, RFC Editor; 2012. <http://www.rfc-editor.org/rfc/rfc6749.txt>.

175.Maler E, Reed D. The venn of identity: Options and issues in federated identity management. IEEE Secur Priv. 2008; 6(2):16–23.

[Article](https://doi.org/10.1109/MSP.2008.50)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=The venn of identity: Options and issues in federated identity management&journal=IEEE Secur Priv&volume=6&issue=2&pages=16-23&publication_year=2008&author=Maler,E&author=Reed,D)

176.Naik N, Jenkins P. Securing digital identities in the cloud by selecting an apposite federated identity management from saml, oauth and openid connect. In: 2017 11th International Conference on Research Challenges in Information Science (RCIS). Piscataway: IEEE: 2017. p. 163–74.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=2017 11th International Conference on Research Challenges in Information Science (RCIS)&publication_year=2017&author=Naik,N&author=Jenkins,P)

177.OASIS. Authentication context for the oasis security assertion markup language (saml) v2.0. 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>.

178.Paci F, Ferrini R, Musci A, Jr KS, Bertino E. An interoperable approach to multifactor identity verification. Computer. 2009; 42(5):50–7.

[Article](https://doi.org/10.1109/MC.2009.142)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=An interoperable approach to multifactor identity verification&journal=Computer&volume=42&issue=5&pages=50-7&publication_year=2009&author=Paci,F&author=Ferrini,R&author=Musci,A&author=Jr,KS&author=Bertino,E)

179.Pöhn D, Metzger S, Hommel W. Géant-trustbroker: Dynamic, scalable management of saml-based inter-federation authentication and authorization infrastructures In: Cuppens-Boulahia N, Cuppens F, Jajodia S, El Kalam AA, Sans T, editors. ICT Systems Security and Privacy Protection. Berlin, Heidelberg: Springer Berlin Heidelberg: 2014. p. 307–20.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ICT Systems Security and Privacy Protection&publication_year=2014&author=P%C3%B6hn,D&author=Metzger,S&author=Hommel,W)

180.Zeng D, Guo S, Cheng Z. The web of things: A survey. J Commun. 2011;6(6). <http://ojs.academypublisher.com/index.php/jcm/article/view/jcm0606424438>.

181.The OpenID Foundation. Openid connect core 1.0. 2014. [http://openid.net/specs/openid-connect-core-1\\_0.html](http://openid.net/specs/openid-connect-core-1_0.html).

182.Domenech MC, Comunello E, Wangham MS. Identity management in e-health: A case study of web of things application using openid connect. In: 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom). Piscataway: IEEE: 2014. p. 219–24.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)&publication_year=2014&author=Domenech,MC&author=Comunello,E&author=Wangham,MS)

183.OASIS. Extensible access control markup language (xacml) version 3.0. 2013. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf>.

184.Borges F, Demirel D, Bock L, Buchmann JA, Mühlhäuser M. A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In: ISCC. USA: IEEE: 2014.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=ISCC&publication_year=2014&author=Borges,F&author=Demirel,D&author=Bock,L&author=Buchmann,JA&author=M%C3%BChlh%C3%A4user,M)

185.Borges de Oliveira F. Background and Models. Cham: Springer International Publishing; 2017. p. 13–23.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Background and Models&publication_year=2017&author=Borges de,Oliveira)

186.Borges de Oliveira F. Reasons to Measure Frequently and Their Requirements. Cham: Springer International Publishing; 2017. p. 39–47.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Reasons to Measure Frequently and Their Requirements&publication_year=2017&author=Borges de,Oliveira)

187.Holvast J. The Future of Identity in the Information Society, volume 298 of IFIP Advances in Information and Communication Technology In: Matyáš V, Fischer-Hübner S, Cvrček D, Švenda P, editors. Berlin: Springer Berlin Heidelberg: 2009. p. 13–42.

188.Toshniwal D. Privacy preserving data mining techniques privacy preserving data mining techniques for hiding sensitive data hiding sensitive data: a step towards open data open data. Singapore: Springer Singapore: 2018. p. 205–12.

189.Li N, Li T, Venkatasubramanian S. t-closeness: Privacy beyond k-anonymity and l-diversity. In: 2007 IEEE 23rd International Conference on Data Engineering. USA: IEEE: 2007. p. 106–15.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=2007 IEEE 23rd International Conference on Data Engineering&publication_year=2007&author=Li,N&author=Li,T&author=Venkatasubramanian,S)

190.De Montjoye Y-A, Hidalgo CA, Verleysen M, Blondel VD. Unique in the crowd: The privacy bounds of human mobility. Sci Rep. 2013; 3:1–5.

[Article](https://doi.org/10.1038/srep01376)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Unique in the crowd: The privacy bounds of human mobility&journal=Sci Rep&volume=3&pages=1-5&publication_year=2013&author=De Montjoye,Y-A&author=Hidalgo,CA&author=Verleysen,M&author=Blondel,VD)

191.Borges de Oliveira F. Quantifying the aggregation size. Cham: Springer International Publishing; 2017. p. 49–60.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Quantifying the aggregation size&publication_year=2017&author=Borges de,Oliveira)

192.Gentry C. A Fully Homomorphic Encryption Scheme. Stanford: Stanford University; 2009. AAI3382729.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A Fully Homomorphic Encryption Scheme&publication_year=2009&author=Gentry,C)

193.Borges de Oliveira F. A Selective Review. Cham: Springer International Publishing; 2017. p. 25–36.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=A Selective Review&publication_year=2017&author=Borges de Oliveira,F)

194.Borges de Oliveira F. Selected Privacy-Preserving Protocols. Cham: Springer International Publishing; 2017. p. 61–100.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Selected Privacy-Preserving Protocols&publication_year=2017&author=Borges de Oliveira,F)

195.Borges F, Lara P, Portugal R. Parallel algorithms for modular multi-exponentiation. Appl Math Comput. 2017; 292:406–16.

[MathSciNet](http://www.ams.org/mathscinet-getitem?mr=3542567)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Parallel algorithms for modular multi-exponentiation&journal=Appl Math Comput&volume=292&pages=406-16&publication_year=2017&author=Borges,F&author=Lara,P&author=Portugal,R)

196.Stamm MC, Wu M, Liu KJR. Information forensics: An overview of the first decade. IEEE Access. 2013; 1:167–200.

[Article](https://doi.org/10.1109/ACCESS.2013.2260814)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Information forensics: An overview of the first decade&journal=IEEE Access&volume=1&pages=167-200&publication_year=2013&author=Stamm,MC&author=Wu,M&author=Liu,KJR)

197.Wu M, Quintão Pereira FM, Liu J, Ramos HS, Alvim MS, Oliveira LB. New directions: Proof-carrying sensing — Towards real-world authentication in cyber-physical systems. In: Proceedings of ACM Conf. on Embedded Networked Sensor Systems (SenSys). New York: ACM: 2017.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Proceedings of ACM Conf. on Embedded Networked Sensor Systems (SenSys)&publication_year=2017&author=Wu,M&author=Quint%C3%A3o Pereira,FM&author=Liu,J&author=Ramos,HS&author=Alvim,MS&author=Oliveira,LB)

198.Grigoras C. Applications of ENF analysis in forensic authentication of digital audio and video recordings. J Audio Eng Soc. 2009; 57(9):643–61.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Applications of ENF analysis in forensic authentication of digital audio and video recordings&journal=J Audio Eng Soc&volume=57&issue=9&pages=643-61&publication_year=2009&author=Grigoras,C)

199.Garg R, Varna AL, Hajj-Ahmad A, Wu M. “seeing” enf: Power-signature-based timestamp for digital multimedia via optical sensing and signal processing. TIFS. 2013; 8(9):1417–32.

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=%E2%80%9Cseeing%E2%80%9D enf: Power-signature-based timestamp for digital multimedia via optical sensing and signal processing&journal=TIFS&volume=8&issue=9&pages=1417-32&publication_year=2013&author=Garg,R&author=Varna,AL&author=Hajj-Ahmad,A&author=Wu,M)

200.Satchidanandan B, Kumar PR. Dynamic watermarking: Active defense of networked cyber–physical systems. Proc IEEE. 2017; 105(2):219–40.

[Article](https://doi.org/10.1109/JPROC.2016.2575064)

[Google Scholar](http://scholar.google.com/scholar_lookup?&title=Dynamic watermarking: Active defense of networked cyber%E2%80%93physical systems&journal=Proc IEEE&volume=105&issue=2&pages=219-40&publication_year=2017&author=Satchidanandan,B&author=Kumar,PR)

**本科毕业论文(设计)中期检查表**

|  |  |  |  |
| --- | --- | --- | --- |
| **学 院** | 医学技术学院 | **专 业** | 18级计算机科学与技术专升本 |
| **姓 名** | 胡立哲 | **学 号** | 201812243102012 |
| **指导老师** | 李懿 | **职 称** | 讲师 |
| **合作老师** |  | **职 称** |  |
| **题目** | 相册簿管理系统 | | |
| **计划完成时间** | | 2020 年 5 月 4 日 | |
| **一、现阶段任务落实情况和成效**  已完成UI管理模块的设计与实现；  已完成相册簿模块的设计与实现； | | | |
| **二、后续工作计划、目标和途径**   1. 研究并实现服务端能同时服务多个客户端 2. 学习JDBC编程并应用于服务端 3. 完成用户管理模块的设计与实现 4. 研究一种加密算法并将其应用于用户的密码加密 5. 测试程序，发现和修改bug | | | |
| **三、指导老师意见**    指导老师签名： 年 月 日 | | | |

1. [] 金良磊. 化繁为简，巧用Windows 10自制电子相册[J]. 电脑知识与技术：经验技巧，2019，（7） [↑](#footnote-ref-0)
2. [] 张志成，王鹏非. 基于stm32单片机的电子相册[J]. 电子技术与软件工程，2016，（4） [↑](#footnote-ref-1)
3. [] 陈金立，高超. 基于TFT显示屏的电子相册设计[J]. 自动化技术与应用，2013，（11） [↑](#footnote-ref-2)
4. [] 康志辉，曾伟渊. 电子相册管理系统设计[J]. 电脑编程技巧与维护，2015，（16） [↑](#footnote-ref-3)
5. [] 戴明儒，陆启军. 基于php技术的电子相册系统分析与设计[J]. 计算机光盘软件与应用，2013，（22） [↑](#footnote-ref-4)
6. [] 禹晨，陆洲. 基于java的电子相册系统的可视化开发与应用[J]，2015，（12） [↑](#footnote-ref-5)
7. [] 燕丽红，林志雄，杨星. 基于Windows 7操作系统和Qt技术的电子相册设计[J]. 现代电子技术，2014，（8） [↑](#footnote-ref-6)
8. [] 张伟. Premiere在音乐电子相册上的开发与应用[J]. 教育教学论坛，2019，（21） [↑](#footnote-ref-7)
9. [] [Karim Abouelmehdi](https://link.springer.xilesou.top/article/10.1186/s40537-017-0110-7" \l "auth-1). Big healthcare data: preserving security and privacy[J]. [Journal of Big Data](https://link.springer.xilesou.top/journal/40537),2018, (5) [↑](#footnote-ref-8)
10. [] [Leonardo B. Oliveira](https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0095-2" \l "auth-1). The computer for the 21st century: present security & privacy challenges[J]. [Journal of Internet Services and Applications](https://jisajournal.springeropen.com/),2018(24) [↑](#footnote-ref-9)
11. [] 朱平哲. 计算机网络信息安全中数据加密技术的分析[J]. 电脑知识与技术，2019 （36）：24-25 [↑](#footnote-ref-10)