基于 AES 算法的账号密码管理 APP

张亚娟,韩银雪,刘效洋
(黄河科技学院 信息工程学院,河南 郑州 450063)

摘　要:随着某些软件长时间不用,就会忘记一些账户信息,尤其是用户名和密码。为了解决大量的账户信息容易忘记、被窃取的问题,在研究了文本记录、浏览器自动保存密码、在线用户密码管理、本地化用户密码管理的基础上,开发了一款基于 AES 算法账号密码管理 APP。这款账号密码管理 APP 主要包括用户的登录注册、登录信息的验证、用户对自己的账户和密码的管理等。对于生活中特别重要的账户以及密码,可以对其进行分组管理并单独为该分组设置密码,将重要密码放入该分组,进行双重保护。使用结果表明,这款账号密码管理 APP 不仅能帮助人们更加方便快捷地记录生活中所注册的用户名和密码,而且通过登录验证环节,保证了用户名和密码的安全性,提高了用户账户信息的安全保障性能。

关键词:账号密码;登录验证;AES 加密;SQLite;数据验证
中图分类号:TP391.43　　**文献标识码**:A　　**文章编号**:1673-629X(2019)08-0125-05
doi:10.3969/j.issn.1673-629X.2019.08.024

Account Password APP Based on AES Algorithm

ZHANG Ya-juan, HAN Yin-xue, LIU Xiao-yang
(School of Information Engineering, College of Huanghe Science and Technology, Zhengzhou 450063, China)

Abstract: As some software goes unused for a long time, some account information, especially user names and passwords, gets forgotten. In order to solve the problem that a large amount of account information is easy to forget and stolen, an account and password management APP based on AES algorithm is developed on the basis of studying text records, browser automatic saving passwords, online user password management and localized user password management. This account password management APP mainly includes the login registration of the user, the authentication of login information, the user's management of his account and password. For the accounts and passwords that are particularly important in life, you can group them and set up a password for the group, placing important passwords in the group for double protection. Practice results show that this account password management APP can not only help people to record the registered user name and password in life more conveniently and quickly, but also ensure the security of the user name and password through the login verification, and improve the security performance of user account information.

Key words: account password; login authentication; AES encryption; SQLite; data validation

0　引　言

随着大量的便捷网站和 APP 的应用[1],需要不断地注册账户。然而随着某些软件长时间不用,就会忘记一些账户信息,尤其是用户名和密码。但是记录在本子或电脑上,又是十分不安全而且容易丢失的。所以,有个能保证用户账户信息安全的移动应用来帮用户随时随地管理这些个人账户是必须的。

1　研究进展

随着计算机科学技术的发展,账户密码管理方式主要有以下几种。

1.1　文本记录

将用户的账户信息记录到类似于记事本的文本工具和 word 文档中的方式[2]最为简单。这种方式虽然简单,但数据安全性特别差是最大的缺点,它几乎是将用户的账户信息直接保存在里面,没有一点安全措施。这些文件一旦丢失,用户的账户信息就有被泄露的风险。

1.2　浏览器自动保存密码

如今自动保存密码功能[3]几乎已经被各大浏览

收稿日期:2018-09-12　　**修回日期**:2019-01-15　　**网络出版时间**:2019-03-27
基金项目:河南省基础与前沿技术研究计划项目(162300410193);郑州市科技发展计划项目(20141371);郑州市嵌入式系统应用技术重点实验室资助项目(121PYFZX177)
作者简介:张亚娟(1979-),女,硕士,副教授,研究方向为物联网安全、数据管理技术、网络软件;韩银雪(1994-),女,研究方向为信息安全。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20190327.1624.038.html

器实现。当人们第一次浏览和登录一些网站的时候，用户的账户和登录密码就会被浏览器保存；当用户再一次浏览登录这些网页时，浏览器将会自动给出相关的登录信息，这样就不需要再自己填写账户名和密码[4]，用户就可以很方便地管理和使用账户信息。然则，如果有黑客恶意攻击用户的计算机，就可以获得用户的所有账户信息[5-6]。所以，使用者信息泄露的风险也存在于这种管理方式中。

1.3 在线用户密码管理

在线用户密码管理工具采用的是在云端服务器里面储存用户的账户信息[7]。现在，LastPass 是国内外应用最为广泛的在线用户账号密码管理工具[8]。虽然在很多地方比浏览器有了很大的进步，但是它同样也有安全方面的隐患。假如有人恶意攻击他的服务器，或者盗取人们用户的 LastPass 密码，那么就泄漏了用户的账户信息。因此，用户信息泄漏的危险也容易发生在 LastPass 中。

1.4 本地化用户密码管理

本地化用户密码管理基本解决了在线管理的安全方面的问题，其中最受欢迎的无疑就是 KeePass[9-10]。在将账户信息保存到数据库之前，先用加密类算法对其加密，通过移动端和电脑端本地数据库储存用户的账户信息。这样的话，不管是用户的电脑被攻击，还是有人偷了用户的电脑，他们看到的账户信息也是经过加密的。然而这种管理工具就只能够在用户的某一台电脑或移动端上，非常不便于用户使用[11]。

针对已有的账户密码管理系统存在的各类弊端和安全问题，文中设计了基于安卓平台的账号密码管理 APP。它能够帮助用户存储有关登录网站、应用软件和银行的应用程序的账户名和密码，与此同时，用户还对账户信息分组进行管理，将相应的账户信息存放到相应的分组中，因此不需要用户记住那么多的账户信息，也不用再手动记录繁杂的账户登录信息。

2 轻量加密算法研究

2.1 RS 加密算法

RS[12]是一种分组加密算法。最开始出现的是 RS4，由于它只是对数据进行了加、异或和循环这些最基础的操作，非常容易实现，所以安全性不是很高。因此在这之后，它的设计者又提出了 RS5，相比 RS4 来说，安全性有所提高。就现在来看，RS5 还算安全，并且容易实现，所以有时会有人把它用在传感器等设备上。但在编码时计算复杂度比较大，需要的存储空间会增加[13]，不太适合用在手机端。

2.2 MD5 加密算法

MD5 是一种不可逆的单向加密算法[14]，不管多长的数据，经过 MD5 转换出来的值都是一样长的。另一方面，MD5 的计算方法简单，给定一个字符串，很容易就能计算出它的 MD5 值，但是把一个 MD5 值转换回原来的数字却十分困难。现在 MD5 算法一般用作数字签名、安全访问验证和一致性验证等方面。虽然 MD5 算法本身是不可逆的，但是这并不表示它不能被人破解。现在网络上就有很多破解 MD5 密码的机制，所以总的来说，它的安全性还是不够高。

2.3 AES 加密算法

相比于 DES 算法，AES 算法的加解密速度更快，安全级别更高，并且可以抵抗当前所有的攻击方法[15]。AES 是一种分组密码[16]。顾名思义，就是把明文分成几组，每一组的长度都一样，依次对每组进行加密，直到结束。在 AES 标准规范中，分组的长度只可为 128 位，也就是说，每组必须是 16 个字节（每 8 位一个字节）。

总之，AES 加密算法不仅灵活性好，而且具有安全性高、效率高、容易实现等优点[17]。在这个系统里面，用户所有的密码信息都是先经过加密处理才存储到数据库中的，如图 1 所示。这样就可以保证在数据库中也看不到用户的密码信息，从而使系统的安全性更好。

rowid	id	account	title	rmk	pwd	isdelete	groupofpwd_id
Click here to define a filter							
1	1	12345562	QQ		nFUUvPNjXyFksNRZBtCP6w==	0	3
2	2	135465	淘宝		6/3/ayy+ZwIOpVij+Qxqhw==	0	4
3	3	45687425	消消乐		pQDITaEwfUA1Qier3TpuGA==	0	2
4	4	4534865	京东		LErzpWUw9m7j/dVlM4N8SA==	0	4
5	5	546543165	百度网盘	常用	0jOuwTaixGhBFuLLCF9ypQ==	0	1

图 1 密码加密存储

3 软件设计与实现

3.1 软件功能设计

这款 APP 包括注册、登录、修改密码、分组管理、账户管理、搜索账号等功能。分组管理是对分组的添加、修改、设置以及组内账户的管理，账户管理方面主要包括账户信息的增删改查，账户搜索是根据用户账户信息中的账户标题或者账号为关键字进行搜索。模

块结构如图 2 所示。

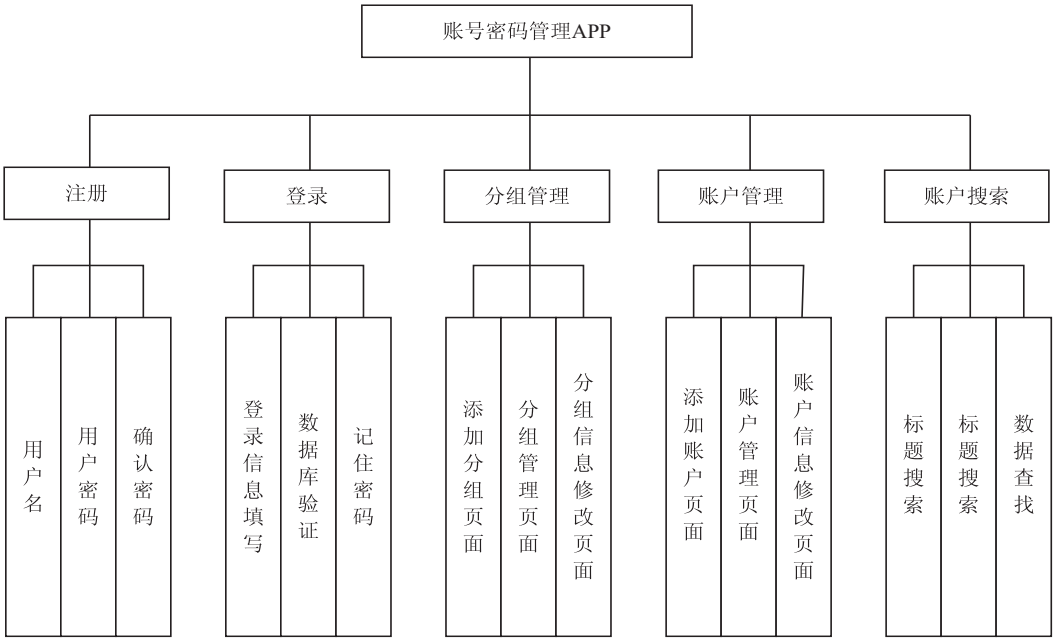

图 2　模块结构

3.2　注册模块

如果是新用户,还没有账户,就可以点击登陆界面的“注册新用户”按钮,进入注册界面。首先,用户需要输入账户名和密码,然后再次确认密码后,点击注册按钮,这时用户名、用户密码和确认密码的内容都会被系统获取。只有当两次密码相同时,系统才会对用户的密码进行 AES 加密,然后把用户新注册的账户信息保存到数据库里面的用户表中去。当用户注册成功以后,系统将会自动跳转回登录页面进行登录。

3.3　登录模块

在创建登录界面之前需要做一些准备工作,主要是如何美化登录界面并准备好美化登录界面时所需要的图片,对登录界面进行美化。

登录界面布局完成后,就是实现登录功能:打开应用,应用程序会先判断当前用户有没有登陆,如果用户已经登录,会直接进入账号管理界面。当用户还没有登陆的时候,程序会给出登陆界面,此时用户需要在登录页面中填写自己的账号和密码,然后点击登录按钮。当用户点击登陆按钮的时候,系统就会自动判断用户名和密码是否为空,只要用户未填写其中的一个信息,系统就会提醒用户名或密码不能为空。只有用户将两个信息都填写完整,即用户名和密码都不为空的时候,系统才会获取用户的账户名和密码。由于这个系统中使用的是本地数据库,所以需要系统根据用户名在 user 表中查询该账户是否存在。如果存在,就查找对应的密码是否存在,如果存在对应的密码,并且与用户输入的密码相同,就登录成功,并跳转到账号管理界面,如图 3 所示。

图 3　用户登录界面

3.4　分组管理模块

分组管理的实现,主要是在 Fragment 中应用 ExpandListview 父元素与子元素的长按事件和其中的点击事件。主要步骤包括两步:第一步,Fragment 里面把 Listview 显示出来。创建一个 Listview,里面是每一个 items 的样式;然后运用 ListFragment 这个类将 Listview 在 Fragment 里面显示出来。ListView 内置在 ListFragment 里面,ListFragment 会自动进行 ListView 的全屏布局。新建一个类继承 ListFragment 之后,把 Fragment 托管到 Activity 里面。

第二步是将 ListView 显示在 Activity 里面。由于 ListView 没有放在 Activity 里面,因此必须把 ListView 控件添加到 Activity 布局里面,同时在 Activity 里面得

到 ListView 实例,然后创建适配器把 ListView 跟数据连接到一起。这个步骤在 Activity 中和上一步的 Fragment 很像,可以参考上一步完成。具体实现效果如图 4 和图 5 所示。

图 4 分组信息界面

图 5 分组管理界面

3.5 账户搜索模块

这个模块的主要功能是根据用户在搜索框里面填写的关键字,在下方实时地显示信息,其实就是 ListView 按照 EditText 搜索框中的关键字实时地把搜索到的账户信息展现出来。所有功能的实现主要包括四个步骤:首先,建立一个布局,在其中放置一个搜索文本框和一个 ListView。然后,创建一个 mData 数据集,用来创建列表视图的适配器。因为在搜索框内容发生改变时,mData 的数据随之变化,所以这里必须有更新操作。

因为要动态改变 ListView 的显示,所以就必须要有 EditText 的内容改变的监听器。当察觉到搜索框内容发生变化时,就用 Handler post 一个 Runnable 做对应的改动。

最后,需要动态更新 ListView,这是最重要的一步。这一步需要根据搜索框的内容在元数据里面查找相符的账户信息,再让它在 ListView 里面显示出来。adapter 有一个 notifyDataSetChanged( ) 方法,这个方法可以在更新数据的时候更新绑定的 ListView。因为第一个就是搜索框,所以一旦开始运行程序,搜索会自动获取焦点。具体效果如图 6 所示。

3.6 修改密码模块

修改密码模块中,主要实现的功能是对密码的修改。首先用户要输入自己的旧密码,以保证在进行修改密码操作的是用户本人,然后输入新密码并对新密码进行确认,最后提交信息。所以在这个页面布局分为两部分,即三个文本框和一个提交按钮。

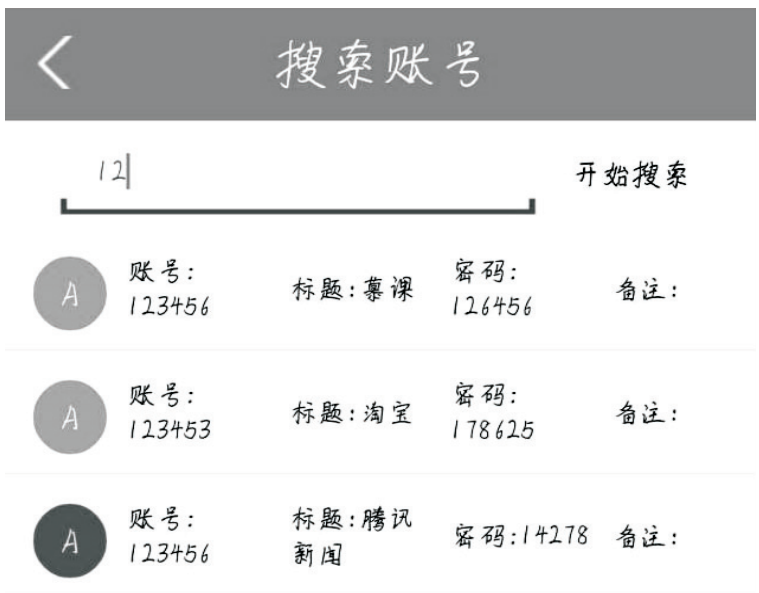

图 6 动态搜索界面

首先创建一个 Layout,里面放三个 Textview,分别是旧密码,新密码和确认密码。然后再放一个 button,就是确认按钮,用于填写完密码修改信息后进行提交。布局完成后需要在 ChangePwdActivity 中进行行为设

置。在每个 EditText 中都需要有相应的提示信息。当某个输入框的信息还没有填写进确认提交的时候,会给出相应的提示,然后通过 et. requestFocus( ) 方法让焦点出现在相应的 EditText 上。当用户提交信息的时候,程序会在数据库中进行查询,判断旧密码是不是正确。旧密码错误或新旧密码不一致都会给出相应的提示语句。

4　结束语

使用 Android Studio 进行开发,运用 Android 数据库框架 LitePal,以及 ExpandListView 控件等,还有夜神模拟器进行模拟,主要实现了账号注册和用户登录、分组管理、账户管理、账户搜索等功能。详细内容包括分组的添加、修改、加密管理、错误提示、账户的信息管理和根据账户标题进行搜索等。

这款账号密码管理 APP,主要的优点包括两方面:一方面是对账户进行了分组管理功能,方便用户管理和查找账户信息;另一方面是对分组进行加密设置,对账户信息进行双重保护,提高了用户信息的安全性,用户可以更加方便和放心地使用它对重要的账户信息进行管理。不足的是,这个项目采用本地存储的方式,虽然增加了账号密码的安全性,但是一旦用户的移动设备丢失,账户信息也将丢失。下一步将考虑在 APP 中设置信息定时导出 PC 机功能,方便用户移动设备的更换。

参考文献:

[1] 张永诺,孙　华,孙子恒. 移动 APP 的应用与发展[J]. 电脑知识与技术,2016,12(2):86-87.

[2] 莫　佳. 基于 Word 文本的信息隐藏系统的设计与实现[J]. 计算机应用与软件,2009,26(12):278-281.

[3] 徐　晏,张代远. 基于浏览器的用户身份识别系统[J]. 计算机技术与发展,2013,23(8):79-82.

[4] 刘长江,万　坚,韩杰思,等. 利用包长特征的浏览器被动识别方法[J]. 西安电子科技大学学报:自然科学版,2017,44(6):144-149.

[5] 孟　辰. 基于代码覆盖的浏览器漏洞利用攻击检测方法[J]. 计算机科学,2011,38(10A):41-43.

[6] 孟永党,蔡　军,何　骏,等. 一种基于 AHP 模型的浏览器漏洞分类方法[J]. 计算机工程与科学,2014,36(11):2137-2141.

[7] 陈　亮,杨　庚,屠袁飞. 混合云环境下基于属性的密文策略加密方案[J]. 计算机应用,2016,36(7):1822-1827.

[8] CUI H T,XU L,WANG G D. Application of last pass force lock-on method to rolling schedule calculation of medium plate[J]. Iron & Steel,2011,46(5):53-55.

[9] MAURYA R K. Using a password manager to access credentials[J]. PC Quest,2015,30(1):59.

[10] STUART R. Read passwords more easily[J]. Computer Active,2013,28(5):46.

[11] 谷　琼,李　杰,龚雄兴. 基于 Android 智能手机的隐私管理系统的设计与实现[J]. 计算机应用与软件,2014,31(1):260-263.

[12] 马　华,曹正文. 基于 RSA 加密算法的叛逆者追踪方案[J]. 西安电子科技大学学报:自然科学版,2004,31(4):611-613.

[13] 胡　冰,杜列波,罗武胜. 基于 RSA+RS 的图像侦察传感器高可靠传输技术研究[J]. 传感器与微系统,2011,30(2):8-10.

[14] 李茂春,王和顺. JAVA WEB 系统用 MD5 算法加密用户口令[J]. 电脑与信息技术,2010,18(5):38-39.

[15] 严利民,李建东. 基于 Impulse C 的 AES 加密算法的仿真与实现[J]. 计算机技术与发展,2012,22(10):184-187.

[16] MOSSA E. Security enhancement for AES encrypted speech in communications[J]. International Journal of Speech Technology,2017,20(1):163-169.

[17] ZEGHID M,MACHHOUT M,KHRIJI L,et al. A modified AES based algorithm for image encryption[J]. International Journal of Computer Science & Engineering,2007,21(1):206-211.