

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

پردیس دانشگاه گیلان

گروه فناوری اطلاعات (تجارت الکترونیک)

طراحی کارت دانشجویی هوشمند

(مورد مطالعه: دانشگاه گیلان)

از

سارا صالحی محبوب

استاد راهنما

دکتر رضا ابراهیمی

استادان مشاور

دکتر شاه بهرامی

دکتر اسدی نژاد

آذر ماه 1390

تقدیم به پدر و مادرم

بر خود واجب می دانم از زحمات جناب دکتر رضا ابراهیمی که با صبر و حوصله خود مرا در انجام این پایان نامه یاری دادند تشکر و قدر دانی را به عمل آورم.

## فهرست مطالب

<b>1</b>	<b>فصل 1: مقدمه</b>
2	1-1- مقدمه
2	2-1- کارت دانشجویی هوشمند
3	3-1- مروری بر پایان نامه
<b>5</b>	<b>فصل 2: کارت های دانشجویی هوشمند</b>
6	1-2- مقدمه
6	2-2- بکارگیری IT در سازمان
6	1-2-2- اثرات بکارگیری IT در سازمان
7	2-2-2- محورهای بکارگیری IT در سازمان
7	3-2-2- پیاده سازی IT در سازمان ها
8	4-2-2- اجرا و بکارگیری IT
9	5-2-2- زیر ساخت نظام فناوری اطلاعات
10	3-2-3- کارایی کارت دانشجویی
	1-3-2- بررسی کاربرد های کارت دانشجویی هوشمند در بعضی دانشگاه های خارج و داخل کشور
13	4-2- پرداخت الکترونیکی
14	1-4-2- تعریف پرداخت الکترونیکی
15	2-4-2- تاریخچه پول و پرداخت
16	3-4-2- روش های پرداخت الکترونیکی
17	5-2- کارت و انواع آن
18	2-5-2- کارت های تماسی
22	3-5-2- کارت های غیر تماسی
<b>24</b>	<b>فصل 3: RFID</b>
25	1-3- مقدمه
25	2-3- تاریخچه RFID
27	3-3- اجزای RFID
29	1-3-3- Tag ها
34	2-3-3- آنتن ها
34	3-3-3- برچسب خوان (قرائنگر یا خواننده)

<b>36</b>	<b>فصل 4: امنیت RFID</b>
37	1-4- مقدمه
37	2-4- بررسی لایه ای حملات روی RFID
39	2-2-4- لایه فیزیکی
43	3-2-4- لایه های کاربردی
45	4-2-4- لایه استراتژیکی
46	5-2-4- لایه حمل و نقل - شبکه
49	3-4- حملات کپی برداری برچسب های RFID
50	1-3-4- توابع کپی ناپذیر فیزیکی و کاربرد آن برای مقاوم سازی در برابر کپی برداری
53	4-4- نتیجه

<b>54</b>	<b>فصل 5: پایگاه داده</b>
55	1-5- مقدمه
55	2-5- بررسی ساختار دانشگاه
59	3-5- پایگاه داده کارت دانشجویی هوشمند
59	1-3-5- تعاریف
61	4-5- شیوه های مورد استفاده برای مدیریت داده ها
62	1-4-5- پردازش فایل به صورت فایلینگ (کلاسیک)
64	2-4-5- سیستم مدیریت پایگاه داده ها DBMS
78	5-5- امنیت شبکه
79	2-5-5- مروری بر مدل TCP/IP
90	3-5-5- امنیت لایه ی انتقال
96	4-5-5- Tunnel
102	6-5- دسته بندی اطلاعات و امنیت آن ها:
103	1-6-5- توکن امنیتی
112	7-5- نتیجه گیری

**113** **فصل 6:**

<b>113</b>	<b>معاونت دانشجویی</b>
114	1-6- مقدمه
114	2-6- ایمن سازی زیر ساخت ها
115	3-6- اجزای معاونت دانشجویی و فرهنگی
120	4-6- تعیین سطح دسترسی
120	1-4-6- بررسی کنترل دسترسی
121	2-4-6- مدل های کنترل دسترسی

129

فصل 7:

129

نتیجه گیری و پیشنهادات

132

مراجع

## فهرست اشکال

- شکل (1-2) بلوک دیاگرام کلی یک ساختار دانشگاهی ..... 17
- شکل (2-2) دسته بندی کارت ها ..... 17
- شکل (3-2) مشخصات فیزیکی کارت هوشمند ..... 21
- شکل (4-2) نحوه عملکرد RFID ..... 23
- شکل (1-3) اجزای سیستم RFID ..... 34
- شکل (1-4) لایه های مختلف RFID ..... 38
- شکل (2-4) دسته بندی حملات RFID ..... 39
- شکل (3-4) انواع PUF ها ..... 51
- شکل (4-4) اجزای اصلی یک برچسب RFID ..... 52
- شکل (5-4) یک برچسب RFID مبتنی بر PUF ..... 53
- شکل (1-5) چارت سازمانی دانشگاه گیلان ..... 56
- شکل (2-5) مثالی برای سلسله مراتب داده در پایگاه داده ..... 60
- شکل (3-5) مثال از پردازش فایلینگ (دانشگاه) ..... 63
- شکل (4-5) نمایش ساده شده مدیریت پایگاه داده ..... 64
- شکل (5-5) مثال از مدیریت پایگاه داده ..... 65
- شکل (6-5) مثالی از مدل داده ای ..... 69
- شکل (7-5) نمایش معماری متمرکز ..... 72
- شکل (8-5) نمای یک سامانه در معماری توزیع شده ..... 72
- شکل (9-5) فرآیند رمزگذاری (محرمانگی داده) ..... 74
- شکل (10-5) رمزنگاری کلید متقارن ..... 75
- شکل (11-5) رمزنگاری نامتقارن ..... 77
- شکل (12-5) تابع Hash ..... 78
- شکل (13-5) مقایسه لایه های OSI و TCP/IP ..... 79
- شکل (14-5) عملکرد تونل ..... 97
- شکل (15-5) انواع توکن ها ..... 104
- شکل (16-5) توکن های منفصل ..... 105
- شکل (1-6) زیرساخت امن برای ایجاد ارتباط در دانشگاه ..... 115
- شکل (2-6) چارت معاونت دانشجویی و فرهنگی ..... 116
- شکل (3-6) مدل سیستم کنترل دسترسی ..... 120
- شکل (4-6) مدل اصلی RBAC ..... 122



شکل (5-6) اجرای RBAC، در معاونت دانشجویی ..... 127

شکل (6-6) اجرای RBAC در معاونت فرهنگی ..... 128

## فهرست جداول

- جدول (1-2) مقایسه دانشگاه ها ..... 14
- جدول (2-2) مقایسه سیستمهای RFID و کارتهای هوشمند تماسی ..... 23
- جدول (1-3) جدول پیشرفت فناوری RFID ..... 26
- جدول (2-3) دسته بندی برچسبهای RFID ..... 32
- جدول (3-3) مقایسه تگها از نظر باند فرکانسی ..... 33
- جدول (1-5) مثالی از موجودیت دانشجو ..... 60
- جدول (2-5) جدول تناظر مفاهیم جدولی و رابطه ای ..... 70
- جدول (3-5) جدول مزایا و معایب مدل ها ..... 71
- جدول (4-5) مقایسه تهدیدات امنیتی در لایه های چهارگانه TCP/IP ..... 86
- جدول (5-5) اهراف امنیتی در منابع شبکه ..... 87
- جدول (6-5) سرویس های امنیتی در لایه های مختلف TCP/IP ..... 87
- جدول (7-5) مکانیزم های امنیتی مربوط به لایه های مختلف TCP/IP ..... 88
- جدول (8-5) مقایسه تجهیزات امنیتی در لایه های مختلف TCP/IP ..... 88
- جدول (1-6) معاونت دانشجویی ACL (Access Control List) ..... 124
- جدول (2-6) ACL (Access List Control) برای معاونت فرهنگی ..... 124

## فهرست علائم اختصاری

AA	اعتبار هویت
ACM	ماتریس کنترل دسترسی
AES	استاندارد رمزگذاری پیشرفته
API	رابط برنامه نویسی
AH	سرآیند هویت
CA	گواهی دیجیتال
CFTP	پروتکل انتقال فایل
DBA	کاربران با نقش مدیریتی
DBMS	سیستم مدیریت پایگاه داده
DES	استاندارد رمزگذاری داده
3DES	استاندارد رمزگذاری داده سه گانه
DOS	حمله جلوگیری از سرویس
DH	دیفی هلمن
DAC	کنترل دسترسی اختیاری
EAS	نظارت مقاله های الکترونیکی
EEPROM	حافظه خواندنی و قابل برنامه ریزی الکتریکی
EPC	کد الکترونیکی محصول
HF	فرکانس بالا
HASH	توابع درهم سازی
HTTP	قرارداد انتقال ابرمتن
HTTPS	پروتکل امن انتقال ابر متن
HDLC	کنترل لینک داده های سطح
HSM	ماژول های سخت افزاری امنیتی
IT	فناوری اطلاعات
ICMP	پروتکل پیغام کنترل اینترنت
IGMP	پروتکل مدیریت گروهی اینترنت

I/O	ورودی/خروجی
L2TP	پروتکل تونل سازی لایه 2
LF	فرکانس پایین
MAC	کنترل دسترسی اجباری
MD5	الگوریتم خلاصه پیام 5
NAT	ترجمه آدرس شبکه
OS	سیستم عامل
PAP	پروتکل تایید گذرواژه
PPP	پروتکل نقطه به نقطه
PPTP	پروتکل تونل نقطه به نقطه
PKI	زیرساخت کلید عمومی
PKI	گواهی کلید عمومی
PUF	توابع غیر قابل کپی برداری فیزیکی
PIN	رمز شناسایی
PROM	حافظه فقط خواندنی قابل برنامه ریزی
PKC	زیرساخت مدیریت امتیاز
RC4	رمزنگاری Revest4
RBAC	کنترل مبتنی بر نقش
RFID	فناوری شناسایی از طریق امواج رادیویی
RAM	حافظه دسترسی تصادفی
ROM	حافظه فقط خواندنی
RSVP	پروتکل ذخیره منبع
SSL	لایه سوکت های ایمن
SHA	الگوریتم هش ایمن
SCTP	پروتکل انتقال کنترل جریان
SMTP	پروتکل انتقال Mail ساده
TIEP	پروتکل تبادل اطلاعات تونل

TLS .....	امنیت لایه انتقال
UHF .....	فرکانس خیلی بالا
UPD .....	پروتکل تبادل اطلاعات
UPC .....	کد جهانی محصول
VPN .....	شبکه خصوصی مجازی
WORM .....	قابلیت یکبار نوشتن و چند بار خواندن
WAN .....	شبکه گسترده بدون سیم

## چکیده

هدف اصلی از طراحی یک کارت دانشجویی هوشمند در دانشگاه، استفاده از بهترین فناوری برای ارائه خدمات، به دانشجویان است که علاوه بر مقرون به صرفه بودن دارای ایمنی مناسب در فضای دانشگاهی باشد. در این پایان نامه، یک مدل امنیتی مناسب برای استفاده از کارت دانشجویی هوشمند غیر تماسی، ارائه می شود. همچنین، امنیت داده های ذخیره شده و امنیت لایه های مختلف شبکه مورد بررسی قرار گرفته شده است و به بررسی حملات روی سیستم RFID و راه حل های ممکن، برای پیشگیری از این حملات، به ویژه، حمله کپی برداری فیزیکی، پرداخته شده است. با استفاده از این کارت ها، دانشگاه می تواند از مزایای زیادی بهره مند شود. از ویژگی های کارت دانشجویی هوشمند، می توان به موارد زیر اشاره نمود:

- پرداخت از طریق کارت که باعث افزایش سرعت و امنیت می شود.
- رفع دشواری حمل پول نقد.
- رفع خطر سرقت وجه نقد.
- داشتن یک رکورد جامع از اطلاعات دانشجویان.
- امکان تخصیص بهینه منابع اشاره کرد.
- کاهش نیروی انسانی و در نتیجه، کاهش خطا
- کاهش هزینه برای دانشگاه
- مدیریت آسان تر منابع
- سرعت بالاتر در ارائه خدمات به دانشجویان
- سهولت در به روز رسانی اطلاعات
- و....

همچنین این طرح باید امکانات دسترسی مرکز های مورد استفاده دانشجویان را مشخص کرده و امکان استفاده همزمان چند منبع از پایگاه اطلاعات دانشجویان را فراهم کند در عین حال امکان توسعه برای نیازمندی های آینده را نیز داشته باشد.

**واژه های کلیدی:** پرداخت الکترونیکی، کارت هوشمند، RFID، RBAC

**Abstract:**

The main purpose of designing a student's smart card in university is the use of the best technology for servicing to students. It is very economically and more safe in university environment. In this thesis, we offer a suitable security model for using the untouchable student intelligence card. Also it is studied on the security of saved data and different layers of network and attacks on the RFID system and its possible solutions in order to prevent these attacks especially physical copyright attacks. By using these cards, the university can enjoy of many advantages. The some characteristics of a student intelligence card are:

- Paying by card that causes to increasing speed and security
- Removing the problems of money carrying
- Having a general record of student information
- The possibility of devoting optimum resources
- Decreasing human power and decreasing error
- Decreasing the cost for university
- Ease resources management
- Having more speed for servicing the students
- Facility in upgrading the information
- And ...

Also this research should determines the availability possibilities of the centers that the students use them and it provide the simultaneous use of different sources in database for students and also it has been the possibilities of development for future requirements.

**Keywords:** E-paying, intelligence card, RFID, RBAC

# فصل 1:

مقدمه



## 1-1- مقدمه

تکنولوژی اطلاعات با محوریت دانش و خردگرایی انسان و اندیشه هایش به منظور بهره برداری از اندیشه و سپردن امور تکراری و غیر خلاق به ماشین و همچنین افزایش کارایی و آزاد سازی مهارت‌های انسانی در دهه های اخیر مورد توجه خاصی قرار گرفته است. از آنجائیکه تکنولوژی اطلاعات به عنوان محور توسعه جوامع و سازمانها مطرح است بنابراین طراحی ساختار آن نیازمند ژرف اندیشی و تأمل همراه با ارائه مدل مناسب و بررسی مدل‌های موجود در سازمان های داخلی و خارجی است. تکنولوژی اطلاعات که از تلاقی الکترونیک، پردازش داده ها و ارتباطات - مخابرات حاصل شده است باعث از میان رفتن فاصله ها و در کنار هم قرار گرفتن کامپیوترها و کاربران و همچنین مکانیزه شدن سیستم های ارتباطی و افزایش ظرفیت های انتقال داده شده است. این امر افزایش سرعت و کیفیت تصمیم گیری و مدیریت کارا را فراهم ساخته است. بکارگیری تکنولوژی اطلاعات در سازمان ها تغییرات بنیادین را در کلیه زمینه ها نوید می دهد همانطوریکه امروزه دنیا را نمی توان بدون صنعت برق در نظر گرفت دنیای امروز را نیز نمی توان بدون فناوری اطلاعات و ارتباطات تصور کرد.

## 1-2- کارت دانشجویی هوشمند

امروزه با پیشرفت روز افزون فناوری اطلاعات، فناوری های نوین همچون فناوری شناسایی از طریق امواج رادیویی (RFID) با استقبال و کاربرد روز افزون در امور مختلف همراه شده است. استفاده از این فناوری، تسریع و تسهیل در ارائه خدمات در دانشگاه ها و موسسات آموزشی را فراهم آورده است. توانایی های این وسیله منجر به ایجاد یک کارت دانشجویی هوشمند شده است که شامل پرونده تحصیلی، کارت شناسایی الکترونیکی، کارت سالن غذاخوری، کارت کتابخانه، کارت خوابگاه و.. می شود، در واقع در اینجا ما مجموعه ای از کارت ها را در یک کارت دانشجویی هوشمند خواهیم داشت. از مزایای استفاده از RFID می توان به دوام بیشتر، دقت بالاتر و سرعت بالاتر این سیستم ها نسبت به سیستم های خودکار دیگر، انعطاف پذیری بالا، کاهش استفاده از نیروی انسانی، امکان تغییر اطلاعات برچسبها در هر زمان و ، کاهش هزینه ها ( کاهش فعالیت های

دستی و افزایش سرعت)، امکان خواندن و نوشتن برچسب‌ها در هر زاویه‌ای و از میان اشیاء (نیاز به دید مستقیم برچسب نیست)، امکان شناسایی منحصر بفرد هر فرد، پایین آمدن نرخ خطا، امکان تهیه گزارشات گوناگون، قابلیت نصب حسگرها به برچسبها (از نوع فعال یا نیمه فعال) و ارسال اطلاعات حسگر، اشاره کرد. انتقال اطلاعات در برچسب‌های RFID، از طریق امواج رادیویی و توسط یک دستگاه قرائتگر حاصل می‌شود. اطلاعات مورد نیاز این سیستم در یک پایگاه داده مرکزی ذخیره و بازیابی می‌گردد، متمرکز بودن داده‌ها سبب شده تا امکان ایجاد یک سیستم امن برای محافظت از آنها بوجود آید. در روش سنتی که هم اکنون در دانشگاه‌ها در حال اجرا است، داده‌ها به صورت جزیره‌ای ذخیره شده‌اند بنابراین به روز رسانی اطلاعات با مشکل مواجه می‌شود و همچنین ایجاد یک محیط امن برای داده‌ها، دشوار و پرهزینه می‌باشد. از طرف دیگر هم اکنون در دانشگاه‌ها از نیروی انسانی برای ارائه خدمات استفاده می‌گردد که خود باعث بروز خطاهای بسیار و صرف وقت بسیار و در نتیجه افزایش هزینه برای دانشگاه می‌شود. استفاده از کارت دانشجویی هوشمند در دانشگاه‌ها سبب سهولت در انجام کارها برای کارکنان و دریافت خدمات بهتر، با کیفیت تر و سریع تر برای دانشجویان می‌شود. همچنین در صورت نیاز به تهیه گزارش از بخش‌های مختلف، این امر به راحتی صورت می‌پذیرد و به روز رسانی اطلاعات سریع تر و راحت تر خواهد بود. علاوه بر این به دلیل کاهش نیروی انسانی، خطا کاهش یافته و در نتیجه هزینه‌ها نیز کاهش می‌یابد. بنابراین مشاهده می‌شود که با صرف یک هزینه اولیه می‌توان از امکانات بهتر، با کیفیت تر و ارزان تر در آینده بهره‌مند گردید.

### 3-1- مروری بر پایان نامه

در این پایان نامه ابتدا به بررسی انواع کارت‌ها و موارد استفاده آن‌ها در دانشگاه‌های مختلف پرداخته شده، سپس با مقایسه مزایا و معایب آن‌ها با هم، مناسب‌ترین نوع کارت برای کارت دانشجویی انتخاب گردیده، که همان RFID می‌باشد. در فصل سوم، RFID معرفی و انواع و اجزای آن نام برده و توضیح داده خواهد شد. فصل چهارم از این پایان نامه در مورد امنیت RFID و حملات تهدید کننده آن و راه‌حل‌های موجود می‌پردازد و به تفصیل PUF<sup>1</sup> که روش

<sup>1</sup> Physically Unclonable Function

پیشگیری از حملات کپی برداری فیزیکی است مورد بررسی قرار می گیرد. در فصل پنجم پایگاه داده معرفی می شود و امنیت داده ها و امنیت شبکه مورد بررسی قرار می گیرد و از میان ابزارها و تجهیزات مختلف مناسب ترین ها، انتخاب و توضیح داده خواهد شد. و در فصل ششم، در مورد بخش های مختلف معاونت دانشجویی و معاونت فرهنگی که سوژه تحقیقاتی، در این پایان نامه است تحقیق به عمل آمده و یک مدل برای کنترل دسترسی آن نشان داده شده است. و در انتها یک جمع بندی از کل پایان نامه و پیشنهاداتی برای آینده ارائه خواهد شد.

## فصل 2:

# کارت های دانشجویی هوشمند