
بسم الله الرحمن الرحيم

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

فهرست اشکال

فهرست جداول

فهرست علائم اختصاری

AA ..... اعتبار هویت
ACM ..... ماتریس کنترل دسترسی
AES ..... استاندارد رمزگذاری پیشرفته
API ..... رابط برنامه نویس
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 در هم 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

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.

واژه‌های 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

فـصل 1 :

مقدمه

1-1- مقدمه

تکنولوژی اطلاعات با محوریت دانش و خردگرایی انسان و اندیشه هایش به منظور بهره بـرداری از اندیشه و سپردن امور تکراری و غیر خلاق بـه ماشـین و همچنـین افـزایش کـارآیی و آزاد سـازی مهارتهای انسانی در دهه های اخیر مورد توجه خاصی قـرار گرفتـه اسـت. از آنجائیکـه تکنولـوژی اطلاعات به عنوان محور توسعه جوامع و سازمانها مطرح است بنابراین طراحی ساختار آن نیازمنـد ژرف اندیشی و تامل همراه با ارائه مدل مناسب و بررسی مدلهای موجود در سازمان های داخلـی و خارجی است. تکنولوژِی اطلاعات که از تلاقی الکترونیک، پردازش داده ها و ارتباطـات - مخـابرات حاصل شده است باعث ازمیان رفتن فاصله ها و در کنار هم قـرار گـرفتن کامپیوترهـا و کـاربران 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 اسـت.بکارگیری تکنولـوژِی 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 اطلاعـات و ارتباطات تصور کرد.

1-2- کارت دانشجویی هوشمند

امروزه با پیشرفت روز افزون فناوری اطلاعات، فنـاوری هـای نـوین همچـون فنـاوری شناسـایی از طریق امواج رادیویی (RFID) با استقبال و کاربرد روز افزون در امور مختلف همـراه شـده اسـت. استفاده از این فناوری، تسریع و تسهیل در ارائه خـدمات در دانشـگاه هـا و موسسـات آموزشـی 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 سـالن غـذاخوری، کـارت کتابخانـه، 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 سـرعت بالاتراین سیستم ها نسبت به سیستم های خودکار دیگر، انعطاف پذیری بـالا، کـاهش اسـتفاده از نیروی انسانی، امکان تغییر اطلاعات برچسبها درهر زمان و ،کاهش هزینه ها (کاهش فعالیت های

دستی و افزایش سرعت)، امکان خواندن و نوشتن برچسب ها در هر زاویه ای و ازمیان اشیاء (نیـاز به دید مستقیم برچسب نیست)، امکان شناسایی منحصر بفرد هر فـرد، پـایین آمـدن نـرخ خطـا، امکان تهیه گزارشات گوناگون، قابلیت نصب حسگرها به برچسبها (از نوع فعـال یـا نیمـه فعـال) و ارسال اطلاعات حسگر، اشاره کرد.انتقال اطلاعات در برچسب های RFID، از طریق امواج رادیویی و توسط یک دستگاه قرائتگر حاصل می‌شود. اطلاعات مورد نیاز ایـن سیسـتم در یـک پایگـاه داده مرکزی ذخیره و بازیابی می گردد، متمرکز بودن داده ها سبب شده تا امکان ایجـاد یـک سیسـتم امن برای محافظت از آنها بوجود آید.در روش سنتی که هم اکنـون در دانشـگاه هـا در حـال اجـرا است، داده هابه صورت جزیره ای ذخیره شده اند بنابر این به روز رسانی اطلاعات با مشکل مواجـه می شود و همچنین ایجاد یک محیط امن برای داده ها، دشوار و پر هزینه می باشد.از طرف دیگـر هم اکنون در دانشگاه ها از نیروی انسانی برای ارائه خدمات استفاده می گردد که خود باعث بـروز خطا های بسیار و صرف وقت بسیار و در نتیجه افزایش هزینه برای دانشگاه می شـود. اسـتفاده از کارت دانشجویی هوشمند در دانشگاه ها سبب سهولت در انجام کارهـا بـرای کارکنـان و دریافـت خدمات بهتر، با کیفیت تر و سریع تر برای دانشجویان می شود. همچنین در صورت نیاز بـه تهیـه گزارش از بخش های مختلف، این امر به راحتی صورت می پذیردو به روز رسانی اطلاعات سریع تر و راحت تر خواهد بود. علاوه بر این به دلیل کاهش نیروی انسانی، خطا کاهش یافتـه و در نتیجـه هزینه ها نیز کاهش می یابد. بنابراین مشاهده می شود که با صرف یک هزینه اولیـه مـی تـوان از امکانات بهتر، با کیفت تر و ارزان تر در آینده بهره مند گردید.

1-3- مروری بر پایان نامه

در این پایان نامه ابتدا به بررسی انواع کارت ها و موارد استفاده آن هـا در دانشـگاه هـای مختلـف پرداخته شده، سپس با مقایسه مزایا و معایب آن ها با هم، مناسب ترین نـوع کـارت بـرای کـارت دانشجویی انتخاب گردیده، که همان RFID می باشد. در فصل سـوم، RFID معرفـی و انـواع 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 راه حـل هـای موجـود مـی پـردازد و بـه تفصـیل PUF[1] کـه روش

[1] Physically Unclonable Function

پیشگیری از حملات کپی برداری فیزیکی است مورد بررسی قرار می گیرد. در فصل پـنجم پایگـاه داده معرفی می شود و امنیت داده ها و امنیت شبکه مورد بررسی قرار می گیرد و از میان ابزار ها و تجهیزات مختلف مناسب ترین ها، انتخاب و توضیح داده خواهد شد. ودر فصل ششـم، در مـورد بخش های مختلف معاونت دانشجویی و معاونت فرهنگی که سوژه تحقیقاتی، در ایـن پایـان نامـه است تحقیق به عمل آمده و یک مدل برای کنترل دسترسی آن نشان داده شده اسـت. و در انتهـا یک جمع بندی از کل پایان نامه و پیشنهاداتی برای آینده ارائه خواهد شد.

فـصل 2 :

کارت های دانشجویی هوشمند