پردیس بین الملل

پایان نامه کارشناسی ارشد

طراحی یک پروتکل امنیتی برای آموزش سیار جهت یادگیری زبان

از

سینا گل محمدی کرجی

استاد راهنما:

دکتر رضا ابراهیمی آتانی

شهریور ماه ۱۳۹۱

پردیس بین الملل

فن آوری اطلاعات (تجارت الکترونیک)

طراحی یک پروتکل امنیتی برای آموزش سیار جهت یادگیری زبان

از

سینا گل محمدی کرجی

استاد راهنما:

دکتر رضا ابراهیمی آتانی

استاد مشاور:

دکتر مهرگان مهدوی

شهریور ماه ۱۳۹۱


بسم الله الرحمن الرحيم

تقدیم به:

پدر و مادر عزیزم که مشوق و پشتوانه محکمی برایم بوده و هستند.

تشکر و قدردانی:

با سپاس بی کران از خداوند مهربان که هر چه دارم از اوست. بهترین فرصت است که از استاد راهنمایم جناب دکتر رضا ابراهیمی آتانی کمال تشکر و قدردانی را بابت تمامی تلاش ها و راهنمایی های ایشان داشته باشم و نیز سپاس گذار زحمات استاد مشاورم جناب دکتر مهرگان مهدوی و استاد گرانقدر دکتر اسدا... شاه بهرامی هستم که در طول تحصیل همواره بنده را مورد لطف و حمایت خویش قرار دادند. در نهایت دست بوس پدر و مادر عزیزم هستم که هیچ تلاش و کوششی را برای موفقیتم از بنده دریغ نکردند.

فهرست مطالب

فهرست اشکال

فهرست جداول

چکیده:

طراحی یک پروتکل امنیتی برای آموزش سیار جهت یادگیری زبان
سینا گل محمدی کرجی

یادگیری سیار کاربرد جدیدی در زمینه فن آوری بی سیم می باشد که امکان یادگیری در هر زمان و هر مکانی را فراهم می آورد. در زمینه آموزش زبان نیز سیستم یادگیری سیار می تواند نقش مهمی را ایفا کند؛ چراکه یادگیرندگان زبان قادر خواهند بود بدون محدودیت زمانی و مکانی به منابع آموزشی دسترسی داشته و به صورت درون خطی مورد سنجش واقع شوند. اما به دلیل ماهیت سیار بودن و نیز منابع محدود دستگاه های سیار، امنیت این سیستم ها مورد توجه قرار گرفته است. اطلاعات مربوط به ارزیابی، بازخورد، رکورد های یادگیرنده، آزمون ها و جواب آنها از اساسی ترین بخش های یادگیری سیار است که باید سرویس های امنیتی در قبال آنها اعمال شود. در این پایان نامه سیر توسعه شیوه های یادگیری تا رسیدن به آخرین حد آن یعنی یادگیری سیار بررسی شده و معرفی جامع و طبقه بندی کاملی از سیستم های یادگیری سیار ارایه شده است. کلیه رسانه های سیار از نسل های مختلف معرفی و از دیدگاه امنیتی مورد ارزیابی قرار گرفته اند و نیز به تشریح پروتکل ها و بستر نرم افزاری های موجود یادگیری سیار پرداخته شده است. در نهایت یک معماری جهت پیاده سازی یک سیستم یادگیری سیار پیشنهاد شده و یک مدل امنیتی طراحی شده است که نواقص امنیتی سیستم های پیشین را مرتفع می سازد. این پروتکل پیشنهادی، سرویس های امنیتی را برای مهم ترین بخش سیستم یادگیری سیار زبان یعنی آزمون درون خطی فراهم آورده و محدودیت های پردازشی و حافظه دستگاه های سیار و نیز سرعت و کارایی بالا را مورد توجه قرار داده است.

روش تحقیق این پایان نامه بر اساس پیاده سازی های موجود از سیستم های یادگیری سیار مختلف بوده و پروتکل پیشنهادی مبتنی بر مدل سازی می باشد.

کلید واژه: یادگیری سیار، معماری، بستر نرم افزاری مستقل از دستگاه، سرویس های امنیتی، رمزنگاری.

Abstract:

Designing a Secure Protocol for Mobile Language Learning
Sina Golmohamadi Karaji

Mobile Learning (M-Learning) is a new application for wireless technology which provides learning in anytime and anywhere. In the field of language learning, it can play a significant role; because it enables mobile learners to access educational materials or contents while on the move, anywhere and anytime and take an online quiz. The information of a learner's assessments, feedback, learner records, homework and the answers of exams is an essential part of M-Learning. Security provision for M-Learning is an open and challenging research problem due to user mobility, limited resources in wireless devices and expensive radio bandwidth.

In this proposal, developement of the learning styles, from distance learning to mobile learning (the last level of learning technology) has been investigated and a comprehensive introduction and complete classification of M-Learning systems is presented. All wireless technologies of various generations have been introduced and evaluated from the security perspective and also the exist protocols and platforms of mobile learning are outlined. Finally, an architecture for implementing an M-learning system and a secure protocol is proposed which overcomes shortcomings of the previous systems. The proposed model provides security services for an online quiz, the most important part of a mobile language learning system. In addition, it considered the performance and high speed of communications and also the proceesing and memory constrains of mobile devices.

This thesis is based on existing methods of implementation of mobile learning systems and the proposed protocol is based on modeling.

Keywords: Mobile Learning (M-Learning), Architecture, Device Independent Platform, Security Services, Cryptography.

فصل ۱:

مقدمه

آموزش و یادگیری یکی از مهم ترین مسایل زندگی امروزی است و همزمان با افزایش جمعیت، رشد و تغییر نیاز ها و درخواست های یادگیرندگان و البته پیشرفت چشمگیر فن آوری اطلاعات و ارتباطات، عرصه بر شیوه های سنتی آموزشی تنگتر شده و این به دلیل محدودیت های مکانی، زمانی، شیوه ها و ابزاری است که آموزش سنتی با آنها مواجه است. با پدیدار شدن آموزش از راه دور و به دنبال آن یادگیری الکترونیکی، توجه سازمان های آموزشی به آن جلب شده و این سازمان ها در صدد بکارگیری فن آوری اطلاعات و ارتباطات در امر آموزش بر آمده اند. با تمام مزایایی که یادگیری الکترونیکی نظیر رفع محدودیت های زمانی و مکانی، کاهش هزینه و تسهیل فرایند آموزش فراهم آورده است، ولی فقدان یک قابلیت سبب ظهور نسل جدیدی از شیوه آموزش و یادگیری به نام یادگیری سیار شده است. این قابلیت، امکان جابه جایی و یادگیری در هر مکان و در هنگام حرکت می باشد که می تواند با حمل یک دستگاه سیار میسر شود. یکی از مهم ترین و پر کاربرد ترین جنبه های سیستم های یادگیری سیار در آموزش زبان است؛ چراکه یادگیرندگان زبان بدون محدودیت زمانی و مکانی قادر خواهند بود به منابع آموزشی دسترسی داشته و در آزمون های درون خطی شرکت کنند. از نقطه نظر دیگر، به دلیل وجود خاصیت جابه جایی و منابع محدود دستگاه های سیار، امنیت سیستم های یادگیری سیار مورد توجه قرار گرفته و در سیستم یادگیری سیار زبان، برقراری سرویس های امنیتی در قبال بخش های مهم این سیستم نظیر آزمون های درون خطی پر اهمیت است. فصول این پایان نامه بدین ترتیب خواهد بود:

فصل ۲ در ارتباط با مرور مقدماتی، پیاده سازی و ارزیابی یادگیری الکترونیکی است. در این فصل به معرفی مفهوم یادگیری الکترونیکی از جنبه های مختلف مثل مشخصه ها، استانداردها و مدل ها می پردازیم. به علاوه، بررسی روی مسایل مهمی شامل پروتکل ها و وظایف، معماری و مدل های یادگیری الکترونیکی خواهیم داشت. همچنین، در مورد سیستم های مدیریت یادگیری در بخش جداگانه ای صحبت خواهیم کرد؛ چرا که این سیستم ها نقش مهمی در برقراری مدیریت و تسهیل فعالیت ها و سرویس های آموزش و یادگیری دارند. به طراحی های آموزشی مختلف برای یادگیری الکترونیکی نیز در قالب بخش مجزایی اشاره خواهد شد. یک نقشه راه[1] توسعه یادگیری الکترونیکی ارایه شده و همچنین موضوعات پایه ای درگیر در هر دو زمینه توسعه و استقرار یادگیری الکترونیکی شرح داده می شوند.

[1] Road Map

جنبه های مختلف پیاده سازی نظیر نیازمندی های مدیریتی و پیاده سازی نواحی حساس فرایند استراتژیک در توسعه یادگیری سیار مورد بررسی قرار خواهد گرفت. به علاوه، بـه مبحـث انتخـاب سیستم عرضه یادگیری الکترونیکی اشاره کرده و یک طبقه بندی از ابزار عرضه ارائه می گردد. در نهایت به بحث در مورد ارزیابی، بازخورد و میانه روی[1] الکترونیکی خواهیم پرداخته می شود.

فصل ۳ شامل معرفی یادگیری سیار و مقایسه آن با نسل های قبلی یادگیری مـی باشـد. در ایـن فصل به بررسی رشد شیوه های یادگیری شـامل یـادگیری از راه دور، یـادگیری الکترونیکـی و در نهایت یادگیری سیار می پـردازیم. انـواع شـیوه هـای آمـوزش از راه دور را بیـان کـرده و گـذار از یادگیری الکترونیکی به یادگیری سیار را بررسی می کنیم و مقایسات جامعی را بین آنها ارایه مـی دهیم که حاصل آن نتایجی است که به امر طراحی سیستم های یادگیری سیار یاری می رسند. در بخش جداگانه ای نیز یک طبقه بندی کلی از مواردی که در یک سیستم یادگیری سیار باید مورد توجه قرار گیرد ارایه می دهیم. در نهایت به مبحث ارزیابی و آزمودن قابلیت استفاده یک سیسـتم یادگیری سیار می پردازیم.

فصل ۴ به بررسی امنیتی زیرساخت های ارتباطی در یادگیری سیار پرداخته است. در این فصـل، یک مروری بر تکنولوژی های ارتباطی سیار مختلف از نسل های مختلف را که در یـادگیری سـیار بکار گرفته شده اند خواهیم داشت. به این صورت که یک معرفی از هـر یـک از تکنولـوژی هـا بـه همراه معماری و پشته پروتکلشان ارایه می دهیم. سپس به رویکرد ها و تکنیک های امنیتـی آنهـا شامل روش های اعمال سرویس های امن می پردازیم. در قسمت پایانی هر بخش نیز، نقاط ضعف هر تکنولوژی و تهدیدات ممکن علیه آنها را بررسی می کنیم. در نهایت، ایـن تکنولـوژی هـا را در قالب جداولی شامل پارامتر های سرویس های امن، نقاط ضعف و تهدیدات ممکن، محدوه پوشش، هزینه بکارگیری و قابلیت بکارگیری در ایران و نیز تکنیک های رمزنگاری و احراز هویـت مقایسـه می کنیم. نتیجه این مقایسه ها این خواهد بود که با توجه به نوع طراحی سامانه یادگیری سـیار و نیازمندی های آن، بتوان تکنولوژی مناسبی که این نیازمندی ها و سرویس های امنیتی مورد نیاز را تامین می کند، اتخاذ کرد.

فصل ۵ پروتکل ها و بستر نرم افزاری های موجود یادگیری سیار و مرتبط با معماری پیشنهادی را شامل می شود. در این فصل به بررسی و معرفی پروتکل های موجود یادگیری سیار می پردازیم.

[1] Moderation

پروتکلی که به صورت جامع ارایه داده شده و نواقص سیستم های قبلی را پوشش داده و با عنوان طراحی و پیاده سازی یک بستر نرم افزاری یادگیری سیار مستقل از دستگاه ارایه داده شده است را به صورت تقصیلی تر شرح می دهیم؛ چراکه این بستر نرم افزاری در معماری پیشنهادی به کار گرفته شده و مدل امنیتی پیشنهادی برای آزمون درون خطی روی این بستر نرم افزاری ارایه می شود. طراحی و پیاده سازی یادگیری سیار زبان انگلیسی را معرفی کرده و در نهایت به بررسی پروتکلی جدیدی در ارتباط امنیت یادگیری سیار می پردازیم.

فصل ۶ شامل معماری و پروتکل امنیتی پیشنهادی برای یادگیری سیار زبان می باشد. در این فصل، با توجه به بستر نرم افزاری های یادگیری سیار موجود، یک معماری سه لایه ای برای سیستم یادگیری سیار زبان پیشنهاد شده و یک پروتکل امنیتی جهت اعمال سرویس های امنیتی طراحی شده است. این پروتکل، سرویس های امنیتی را برای مهم ترین بخش سیستم یادگیری سیار زبان یعنی آزمون درون خطی فراهم آورده و محدودیت های پردازشی و حافظه دستگاه های سیار و نیز سرعت و کارایی بالا را مورد توجه قرار داده است. در انتها نیز، بستر نرم افزاری مورد استفاده، معماری و پروتکل امنیتی پیشنهادی از دیدگاه های مختلف مورد ارزیابی قرار گرفته اند.

فصل ۷ به جمع بندی کلی و پیشنهاد ها برای فعالیت های آتی می پردازد. اهداف، دست آورد ها و نو آوری های این پایان نامه در این فصل بیان شده و پیشنهاد هایی برای ادامه یا تکمیل پروژه ارایه می گردد.

فصل ۲:

مرور مقدماتی بر یادگیری الکترونیکی،

پیاده سازی و ارزیابی آن

۲-۱- معرفی یادگیری الکترونیکی

مفهوم یادگیری الکترونیکی[1] اخیرا در ادبیات و مفاهیم مربوط بـه یـادگیری در محـیط فـن آوری اطلاعات و ارتباطات[2] شهرت یافته است. یادگیری الکترونیکی در واقع بکارگیری ICT در یادگیری به منظور کسب، ذخیره و پردازش اطلاعات می باشد و در آن یادگیرنده به صورت واقعی مشـاهده، تفکر، ارتباط، کسب و تبادل اطلاعات کرده و تجربیات را با استفاده از "دانستن-چگونگی" در هـر روز کاری و فعالیت های اوقات فراغت مبادله می کند [۱]. یادگیری الکترونیکی به طور معمول، به استفاده ارادی از اطلاعات شبکه شده و فن آوری ارتباطات در آموزش و یادگیری اشاره مـی کنـد. رشد علاقمندی در یادگیری الکترونیکی از چندین جهت ناشی می شـود کـه ایـن جهـات شـامل سازمان هایی هستند که به صورت سنتی، برنامه های آموزشی از راه دور را در تنظیم حالت یگانه، دوگانه و یا ترکیبی پیشنهاد کـرده انـد. آنهـا همکـاری یـادگیری درون خطـی را در برنامـه هـای موجودشان به عنوان یک توسعه منطقی فعالیت های آموزشی از راه دور می بینند. از سوی دیگـر، بخش سازمانی در یادگیری الکترونیکی به عنوان راهی برای توجیه منطقی هزینه های فعالیت های آموزشی کارکنان داخلی، مورد توجه قرار گرفته است. یادگیری الکترونیکی جهت برقراری سازمان های آموزشی پردیس–محور به همان خوبی مورد توجه است. آنها به یادگیری الکترونیکی به عنوان راهی جهت بهبود دستیابی به برنامه هایشان و نیز راهی جهت اتصال به رشـد جایگـاه ویـژه بـازار، نگاه می کنند. رشد یادگیری الکترونیکی مستقیما به افزایش دسترسـی بـه فـن آوری اطلاعـات و ارتباطات به خوبی کاهش هزینه آن بستگی دارد. ظرفیت فـن آوری اطلاعـات و ارتباطـات جهـت پشتیبانی آموزش و یادگیری برپایه منابع چندرسانه ای نیـز بـه رشـد میـزان توجـه بـه یـادگیری الکترونیکی مرتبط است. تعداد معلمانی که از ICT جهت پشتیبانی آموزششان استفاده مـی کننـد رو به افزایش است. جمعیت فعلی دانش آموزان که اغلب با عنوان "نسل نتی" خطاب می شـوند و از ICT در تجربیات آموزشیشان استفاده می کنند نیز در حال افزایش است.

---

[1] E-Learning

[2] Information & Communication Technology (ICT)

سازمان های آموزشی نیز مزایایی را در دسترس ساختن برنامه هایشان به وسیله رنجی از مکان های توزیع شده شامل پردیس، خانه و دیگر جوامع یادگیری و مراکز منابع، می بینند. با وجود این سطح از علاقه مندی در یادگیری الکترونیکی، محدودیت هایی نیز وجود دارد [۱]. مانع اصلی رشد یادگیری الکترونیکی، کمبود دسترسی به زیرساخت فن آوری مورد نیاز می باشد که بدون آن یادگیری الکترونیکی میسر نخواهد بود. زیرساخت فن آوری ضعیف و غیر موثر ممکن است تجربیات ناخوشایندی را برای معلمان، دانش آموزان و در کل تجربه یادگیری داشته باشد. همزمان با افزایش هزینه های سخت افزاری و نرم افزاری، هزینه های دیگری نیز وجود خواهد داشت که معمولا در استقرار ریسک ها و اقدامات یادگیری الکترونیکی در نظر گرفته نشده اند. مهمترین آنها شامل هزینه های پشتیبانی زیرساخت و نگهداری آن و آموزش مناسب کارکنان به منظور توانمند ساختن آنها جهت ایجاد بیشترین فن آوری می باشد. به علاوه یادگیری الکترونیکی فرصت هایی را جهت طراحی محیط های یادگیری که در محتوای یادگیری معتبر بوده و همچنین مشکل–محور باشند، فراهم می کند و این امر به منظور آماده کردن دانش آموزان با تجربیات "یادگیری با انجام دادن" می باشد [۲].

۲-۱-۱- مشخصه های یادگیری الکترونیکی

در این بخش ، قصد داریم تنها به بحث در مورد خصوصیات حیاتی و منحصر به فرد تکنولوژی های یادگیری الکترونیکی بپردازیم.

۲-۱-۱-۱- انعطاف پذیری یادگیری الکترونیکی

یک صفت کلیدی ICT قابلیت آن در قادر ساختن دسترسی منعطف به اطلاعات و منابع می باشد. دسترسی منعطف به دستیابی و استفاده از اطلاعات و منابع در یک زمان، مکان و گام اشاره دارد که در قیاس با معلمان و سازمان های آموزشی، مناسب یادگیرندگان مستقل می باشد. مفهوم آموزش از راه دور بر پایه اصول دسترسی منعطف بنا نهاده شده بود. این امر به یادگیرندگان راه دور که معمولا به صورت تمام وقت یا پاره وقت آموزش می بینند، این امکان را می دهد که در