



دانشگاه تهران

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

پرديس بين الملل  
فن آوري اطلاعات (تجارت الکترونيك)

# طراحی يك پروتکل امنیتی برای آموزش سیار جهت یادگیری زبان

از  
سینا گل محمدی کرجی

استاد راهنما:  
دکتر رضا ابراهیمی آتانی

استاد مشاور:  
دکتر مهرگان مهدوی

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِيْمِ

## 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 راهنماییم 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 اسدآ... 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

### ۱ ..... فصل ۱: مقدمه

### ۵ ..... فصل ۲: مرور مقدماتی بر یادگیری الکترونیکی، پیاده سازی و ارزیابی آن

۶ ..... ۲-۱- معرفی یادگیری الکترونیکی
۷ ..... ۲-۱-۱- مشخصه های یادگیری الکترونیکی
۷ ..... ۲-۱-۱-۱- انعطاف پذیری یادگیری الکترونیکی
۹ ..... ۲-۱-۱-۲- دسترسی الکترونیکی به منابع بربایه چندرسانه ای و ابر رسانه ای
۹ ..... ۲-۱-۲- استانداردهای یادگیری الکترونیکی
۱۱ ..... ۲-۱-۳- مدل های یادگیری الکترونیکی
۱۲ ..... ۲-۲- پروتکل ها و جایگاه یادگیری درون خطی
۱۴ ..... ۲-۳- معماری ها و مدل های یادگیری الکترونیکی
۱۵ ..... ۲-۳-۱- مدل عملیاتی
۱۶ ..... ۲-۳-۲- معماری سرویس
۱۸ ..... ۲-۳-۳- محیط یادگیری الکترونیکی برای یک پرتال آموزشی
۲۱ ..... ۴-۲- سیستم های مدیریتی یادگیری درون خطی (LMS)
۲۲ ..... ۴-۳-۱- پشتیبانی استاندارد های پدیدار شده
۲۳ ..... ۴-۳-۲- محدودیت های سیستم های مدیریت کنونی
۲۴ ..... ۴-۳-۳- انتخاب یک سیستم مدیریت یادگیری
۲۵ ..... ۵-۲- طراحی های آموزشی برای یادگیری الکترونیکی
۲۷ ..... ۶-۲- توسعه و استقرار یادگیری الکترونیکی
۳۰ ..... ۷-۲- پیاده سازی یادگیری الکترونیکی
۳۲ ..... ۸-۲- انتخاب سیستم ارایه یا انتقال یادگیری الکترونیکی
۳۴ ..... ۹-۲- ارزیابی، بازخورد و میانه روی الکترونیکی
۳۴ ..... ۹-۱- ارزیابی دست آوردهای یادگیری
۳۵ ..... ۹-۲- روش های ارزیابی
۳۷ ..... ۹-۳- تهیه بازخورد
۳۸ ..... ۹-۴- میانه روی در یادگیری درون خطی

### ۳۹ ..... فصل ۳: معرفی یادگیری سیار و مقایسه آن با نسل های پیشین یادگیری

۴۰ ..... ۳-۱- معرفی یادگیری سیار
۴۱ ..... ۳-۱-۱- جایگاه و مدل لایه ای یادگیری سیار
۴۳ ..... ۳-۲- استانداردهای یادگیری سیار
۴۶ ..... ۳-۲- ۳- یادگیری از راه دور

۳-۳	- گذار از یادگیری الکترونیکی به یادگیری سیار.....	۴۸
۴-۳	- طبقه بندی عمومی از سیستم های یادگیری سیار.....	۵۱
۵-۳	- ارزیابی یادگیری سیار.....	۵۸

<b>۶۱</b>	<b>فصل ۴: بررسی امنیتی زیرساخت های ارتباطی در یادگیری سیار</b>
۶۲	- مقدمه.....
۶۲	- تکنولوژی های ارتباطی بی سیم از نسل های مختلف ارتباطی.....
۶۴	- طبقه بندی تکنولوژی های ارتباطی یادگیری سیار.....
۶۶	- مقایسه فن آوری های ارتباطی در یادگیری سیار و نتیجه گیری.....

<b>۷۰</b>	<b>فصل ۵: پروتکل و بستر نرم افزاری های مرتبه</b>
۷۱	- مقدمه.....
۷۲	- معرفی سیستم های یادگیری سیار رایج .....
۷۲	- ۱-۲-۵ محیط یادگیری الکترونیکی و ارتباطی بی سیم (WELCOME)
۷۳	- ۲-۲-۵ موتور یادگیری سیار (MLE).....
۷۳	- ۳-۲-۵ Mobile ELDIT .....
۷۵	- ۴-۲-۵ محیط یادگیری تعاملی سیار-محور (MOBILE).....
۷۶	- ۵-۲-۵ یک سیستم یادگیری سیار وفق پذیر.....
۷۷	- ۶-۲-۵ بستر نرم افزاری یادگیری سیار (MobiLP).....
۷۸	- ۳-۵ یک بستر نرم افزاری مستقل از دستگاه برای یادگیری سیار .....
۸۰	- ۱-۳-۵ خصوصیات بستر نرم افزاری مستقل از دستگاه یادگیری سیار .....
۸۱	- ۲-۳-۵ معماری بستر نرم افزاری یادگیری سیار مستقل از دستگاه .....
۸۵	- ۳-۳-۵ کلاس بندی بستر نرم افزاری یادگیری سیار مستقل از دستگاه .....
۸۶	- ۴-۵ طراحی و پیاده سازی یادگیری سیار زبان انگلیسی .....
۸۷	- ۱-۴-۵ طراحی بسته منبع یادگیری سیار زبان انگلیسی .....
۸۸	- ۲-۴-۵ طراحی بسته منبع .....
۸۸	- ۱-۲-۴-۵ پیمانه سازی منبع یادگیری .....
۸۹	- ۲-۲-۴-۵ طراحی محتوا پیمانه .....
۹۰	- ۳-۲-۴-۵ پیوستگی ضمنی میان پیمانه ها .....
۹۱	- ۴-۲-۴-۵ محتوا واقع شده .....
۹۲	- ۳-۴-۵ طراحی تعاملات در یادگیری سیار زبان انگلیسی .....
۹۲	- ۱-۳-۴-۵ طراحی واسط .....
۹۳	- ۲-۳-۴-۵ طراحی سیستم پرسش و پاسخ .....
۹۴	- ۴-۴-۵ پیاده سازی سیار زبان انگلیسی .....
۹۵	- ۵-۵ پروتکل امنیتی برای یادگیری سیار .....
۹۷	- ۱-۵-۵ نیازمندی های امنیتی .....

۹۸	۲-۵-۵-۱-۲-۵-۵	- اصول مقدماتی ..... - نماد ها .....
۹۸	۲-۲-۵-۵	- زیرساخت شبکه .....
۹۹	۳-۵-۵	- طراحی پروتکل .....
۹۹	۴-۵-۵	- تحلیل امنیتی .....
۱۰۱	۵-۵-۵	- مقایسه پروتکل های مرتبط NAAP با پروتکل ..... .....

۱۰۵	<b>فصل ۶: معماری و پروتکل امنیتی پیشنهادی برای یادگیری سیار زبان</b>
۱۰۶	۱-۶- مقدمه .....
۱۰۶	۲-۶- محتویات یا منابع یادگیری زبان .....
۱۰۸	۱-۲-۶- دسترسی به محتویات از دیدگاه یادگیرنده ..... .....
۱۱۰	۲-۲-۶- دسترسی به محتویات از دیدگاه مدرس .....
۱۱۰	۱-۲-۲-۶- ایجاد یک کوییز از ابتدا .....
۱۱۱	۲-۲-۲-۶- ایجاد یک کوییز از پایگاه دانش .....
۱۱۲	۳-۲-۲-۶- ایجاد یک کوییز از فایل XML کوییز موجود .....
۱۱۲	۳-۶- معماری پیشنهادی برای سیستم یادگیری سیار زبان .....
۱۱۴	۴-۶- امنیت فن آوری های به کار گرفته شده جهت انتقال محتویات .....
۱۱۴	۱-۴-۶- پروتکل انتقال فرمان (HTTP) و به کارگیری HTTPS .....
۱۱۷	۲-۴-۶- پروتکل کاربردی بی سیم (WAP 1.x و WAP 2.x) .....
۱۱۷	۱-۲-۴-۶- WAP 1.x -
۱۲۰	۲-۲-۴-۶- WAP 2.x -
۱۲۳	۳-۴-۶- مشکلات امنیتی WAP .....
۱۲۳	۱-۳-۴-۶- مشکل امنیتی درگاه WAP .....
۱۲۴	۲-۳-۴-۶- مشکلات امنیتی WTLS .....
۱۲۵	۵-۶- پروتکل امنیتی پیشنهادی .....
۱۲۵	۱-۵-۶- فرضیات پروتکل امنیتی پیشنهادی .....
۱۲۶	۲-۵-۶- رمزنگاری آزمون در سیستم یادگیری سیار زبان .....
۱۲۷	۱-۲-۵-۶- الگوریتم رمزنگاری RC4 .....
۱۲۹	۲-۲-۵-۶- تابع درهم ساز MD5 .....
۱۳۱	۳-۲-۵-۶- تابع درهم ساز تولید کلید .....
۱۳۲	۶-۶- فرایند کارکرد سیستم .....
۱۳۴	۷-۶- ارزیابی و نتیجه گیری .....
۱۳۴	۱-۷-۶- ارزیابی بستر نرم افزاری یادگیری سیار مستقل از دستگاه به کار گرفته شده .....
۱۳۶	۲-۷-۶- ارزیابی معماری پیشنهادی برای یادگیری سیار زبان .....
۱۳۷	۳-۷-۶- ارزیابی پروتکل امنیتی پیشنهادی برای یادگیری سیار زبان .....

## فصل ۷: جمع بندی و پیشنهاد ها

۱۳۹	
۱۴۰	۱-۷ مقدمه
۱۴۰	۲-۷ جمع بندی
۱۴۱	۳-۷ پیشنهاد ها

۱۴۳

مراجع

۱۴۷

پیوست ها

## فهرست اشکال

شکل (۱-۲) چارچوبی برای روش های یادگیری ..... ۱۴
شکل (۲-۲) مدل عملیاتی سیستم یادگیری الکترونیکی ..... ۱۶
شکل (۳-۲) معماری سرویس سیستم یادگیری الکترونیکی ..... ۱۷
شکل (۴-۲) معماری یک محیط عمومی یادگیری الکترونیکی ..... ۱۹
شکل (۵-۲) دیاگرام جریان داده از سمت کاربر تا LCMS ها و بالعکس ..... ۲۰
شکل (۶-۲) ساختار LCMS توسعه داده شده ..... ۲۰
شکل (۷-۲) طرح توسعه یادگیری الکترونیکی ..... ۲۸
شکل (۱-۳) مدل لایه ای یادگیری سیار، متناظر با لایه های مدل مرجع TCP/IP ..... ۴۱
شکل (۲-۳) جایگاه یادگیری سیار ..... ۴۲
شکل (۳-۳) مقایسه پشته پروتکل های WAP و اینترنت ..... ۴۳
شکل (۴-۳) یادگیری الکترونیکی توسعه یافته با محاسبات سیار ..... ۵۱
شکل (۵-۳) طبقه بندی کلی از سیستم های یادگیری سیار ..... ۵۴
شکل (۱-۴) تکنولوژی های ارتباطی بی سیم از نسل های مختلف ..... ۶۴
شکل (۲-۴) طبقه بندی تکنولوژی های ارتباطی در یادگیری سیار ..... ۶۵
شکل (۱-۵) مدل یادگیری سیار ..... ۷۸
شکل (۲-۵) مدل ماشین یادگیری سیار ..... ۷۸
شکل (۳-۵) معماری بستر نرم افزاری یادگیری سیار مستقل از دستگاه ..... ۸۲
شکل (۴-۵) مدل مشخصات بستر نرم افزاری یادگیری سیار مستقل از دستگاه ..... ۸۶
شکل (۵-۵) پیمانه سازی منابع سیستماتیک ..... ۸۸
شکل (۶-۵) ساختار منابع یادگیری ..... ۹۰
شکل (۷-۵) اشکال مختلف رسانه محتوای یادگیری ..... ۹۲
شکل (۸-۵) ساختار سیستم پرسش و پاسخ (Q&A) ..... ۹۳
شکل (۹-۵) ساختار سیستم یادگیری سیار زبان انگلیسی ..... ۹۴
شکل (۱۰-۵) پروتکل NAAAP ..... ۱۰۱
شکل (۱-۶): معماری پیشنهادی سیستم یادگیری سیار زبان ..... ۱۱۳
شکل (۲-۶): شمای کلی تولید و ارسال آزمون ..... ۱۲۷
شکل (۳-۶): عملکرد تابع درهم ساز MD5 ..... ۱۳۱
شکل (۴-۶): فرایند تولید کلید جهت استفاده در رمزنگاری RC4 ..... ۱۳۲
شکل (۵-۶): فرایند آزمون در سیستم یادگیری سیار زبان ..... ۱۳۳

## فهرست جداول

جدول (۱-۲) جنبه های کلیدی در پیاده سازی یادگیری الکترونیکی ..... ۳۱
جدول (۲-۲) مزایا و معایب روش های ارایه در یادگیری الکترونیکی ..... ۳۲
جدول (۳-۲) کلاس بندی ابزار ارایه در یادگیری الکترونیکی ..... ۳۳
جدول (۱-۳) مقایسه جامع محیط یادگیری الکترونیکی و یادگیری سیار ..... ۴۹
جدول (۱-۴) مقایسه سرویس های امنیتی پشتیبانی شده ..... ۶۷
جدول (۲-۴) نقاط ضعف و تهدیدات ممکن ..... ۶۷
جدول (۳-۴) پهنهای باند پشتیبانی شده ..... ۶۸
جدول (۴-۴) هزینه به کارگیری ..... ۶۸
جدول (۴-۵) محدوده پوشش و قابلیت بکارگیری در ایران ..... ۶۹
جدول (۶-۴) تکنیک های رمزنگاری و احراز هویت ..... ۶۹
جدول (۱-۵) : مقایسه سه پروتکل AUTHMAC_DH، KAAP و NAAP ..... ۱۰۳

## 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, development 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 processing and memory constraints 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 برآمده 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 مجازی اشاره خواهد شد. یک نقشه راه<sup>۱</sup> توسعه یادگیری الکترونیکی ارایه شده و همچنین موضوعات پایه ای در گیر در هر دو زمینه توسعه و استقرار یادگیری الکترونیکی شرح داده می شوند.

<sup>1</sup> Road Map

جنبه های مختلف پیاده سازی نظری نیازمندی های مدیریتی و پیاده سازی نواحی حساس فرایند استراتژیک در توسعه یادگیری سیار مورد بررسی قرار خواهد گرفت. به علاوه، به مبحث انتخاب 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<sup>۱</sup> الکترونیکی خواهیم پرداخته می شود.

**فصل ۳** شامل معرفی یادگیری سیار و مقایسه آن با نسل های قبلی یادگیری می باشد. در این فصل به بررسی رشد شیوه های یادگیری شامل یادگیری از راه دور، یادگیری الکترونیکی و در نهایت یادگیری سیار می پردازیم. انواع شیوه های آموزش از راه دور را بیان کرده و گذار از یادگیری الکترونیکی به یادگیری سیار را بررسی می کنیم و مقایسات جامعی را بین آنها ارایه می دهیم که حاصل آن نتایجی است که به امر طراحی سیستم های یادگیری سیار یاری می رساند. 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 سیستم یادگیری سیار می پردازیم.

**فصل ۴** به بررسی امنیتی زیرساخت های ارتباطی در یادگیری سیار پرداخته است. در این فصل، یک مروری بر تکنولوژی های ارتباطی سیار مختلف از نسل های مختلف را که در یادگیری سیار بکار گرفته شده اند خواهیم داشت. به این صورت که یک معرفی از هر یک از تکنولوژی ها به همراه معماری و پشته پروتکلشان ارایه می دهیم. سپس به رویکرد ها و تکنیک های امنیتی آنها 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، این تکنولوژی ها در قالب جداولی شامل پارامتر های سرویس های امن، نقاط ضعف و تهدیدات ممکن، محدوده پوشش، هزینه بکارگیری و قابلیت بکارگیری در ایران و نیز تکنیک های رمزنگاری و احراز هویت مقایسه می کنیم. نتیجه این مقایسه ها این خواهد بود که با توجه به نوع طراحی سامانه یادگیری سیار 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.

<sup>1</sup> 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 تفصیلی 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 انتهای 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 آوردها و نوآوری های این پایان نامه در این فصل بیان شده و پیشنهاد هایی برای ادامه یا تکمیل پژوهش ارایه می گردد.

## **فصل ۲:**

**مرور مقدماتی بر یادگیری الکترونیکی،**

**پیاده سازی و ارزیابی آن**

## ۱-۲- معرفی یادگیری الکترونیکی

مفهوم یادگیری الکترونیکی<sup>۱</sup> اخیرا در ادبیات و مفاهیم مربوط به یادگیری در محیط فن آوری اطلاعات و ارتباطات<sup>۲</sup> 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 مشاهده، تفکر، ارتباط، کسب و تبادل اطلاعات کرده و تجربیات را با استفاده از "دانستن چگونگی" در هر 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 می کند. رشد علاقمندی در یادگیری الکترونیکی از چندین جهت ناشی می شود که این جهات شامل سازمان هایی هستند که به صورت سنتی، برنامه های آموزشی از راه دور را در تنظیم حالت یگانه، دوگانه و یا ترکیبی پیشنهاد کرده اند. آنها همکاری یادگیری درون خطی را در برنامه های موجودشان به عنوان یک توسعه منطقی فعالیت های آموزشی از راه دور می بینند. از سوی دیگر، 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 پر迪س -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 رشد جایگاه ویژه بازار، نگاه می کنند. رشد یادگیری الکترونیکی مستقیماً به افزایش دسترسی به فن آوری اطلاعات و ارتباطات به خوبی کاهش هزینه آن بستگی دارد. ظرفیت فن آوری اطلاعات و ارتباطات جهت پشتیبانی آموزش و یادگیری برپایه منابع چندرسانه ای نیز به رشد میزان توجه به یادگیری الکترونیکی مرتبط است. تعداد معلمانی که از ICT جهت پشتیبانی آموزششان استفاده می کنند رو به افزایش است. جمعیت فعلی دانش آموزان که اغلب با عنوان "نسل نتی" خطاب می شوند و از ICT در تجربیات آموزشیشان استفاده می کنند نیز در حال افزایش است.

<sup>1</sup> E-Learning

<sup>2</sup> Information & Communication Technology (ICT)

سازمان های آموزشی نیز مزایایی را در دسترس ساختن برنامه هایشان به وسیله رنجی از مکان های توزیع شده شامل پر迪س، 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 عموماً 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].

## ۱-۱-۲- 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.

## ۱-۱-۱-۲- 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 عموماً به صورت تمام وقت یا پاره وقت آموزش می بینند، این امکان را می دهد که در