دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

گزارش نوشتاری درس روش تحقیق و پژوهش

بررسی کارکرد کارت هوشمند سلامت جایگزین دفترچه های بیمه و خدمات درمانی

نگارش

آرش حاجی صفی

استاد راهنما

دکتر رضا صفابخش

استاد مشاور

دکتر مهدی راستی

مرداد ۱۳۹۹

دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

گزارش نوشتاری درس روش تحقیق و پژوهش

بررسی کارکرد کارت هوشمند سلامت جایگزین دفترچه های بیمه و خدمات درمانی

نگارش

آرش حاجی صفی - ۹۶۳۱۰۱۹

استاد راهنما

دکتر رضا صفابخش

استاد مشاور

دکتر مهدی راستی

مرداد ۱۳۹۹

سپاس گزاری

از پدر و مادر عزیزم که در تهیه این گزارش با لطف بی حدشان مرا یاری کردند، و همینطور استاد گرامی‌ام، دکتر صفابخش، کمال تشکر را دارم و از خداوند منان خواهان طول عمری با برکت برای ایشان هستم.

آرش حاجی صفی

مرداد ۱۳۹۹

چکیده

جابجایی مداوم بیماران و پزشکان، و همچنین وجود گروه های متعدد پزشکی متشکل از پزشکان خصوصی، پزشکان عمومی، بیمارستانها، مراکز درمانی و شرکتهای بیمه مشکلات قابل توجهی در مدیریت اطلاعات پزشکی بیماران ایجاد می کند. به ناچار، این مسئله بر کیفیت خدمات درمانی ارائه شده توسط مراکز نامبرده شده تأثیر می گذارد. فناوری کارت هوشمند که مدتی است معرفی شده و به سرعت در حال تغییر و تحول است، می تواند برای پیاده سازی پرونده های الکترونیکی قابل حمل بیمار جهت حل این مشکل مورد استفاده قرار بگیرد. علاوه بر اطلاعات پزشکی، اطلاعات بیمه نیز می توانند بر روی کارت هوشمند ذخیره شوند و از این طریق ایجاد یک "سیستم هوشمند" را برای مدیریت کارآمد اطلاعات بیمار، تسهیل کنند. در این پژوهش ضمن معرفی انواع کارت هوشمند و پرونده های سلامت الکترونیکی، ویژگی های اصلی معماری و عملکردی این سیستم ارائه می شود. همچنین در قسمت های پایانی به شرح چگونگی حفاظت از "محرمانگی" و "تمامیت" اطلاعات بیمار در چنین سامانه ای پرداخته خواهد شد.

واژه‌های کلیدی:

کارت هوشمند، سلامت الکترونیک، پرونده سلامت الکترونیک، تمامیت و محرمانگی اطلاعات، تهدیدات امنیتی

فهرست مطالب

عنوان صفحه

۱ **مقدمه** ۱

۲ **شناخت کارت‌های هوشمند و دسته‌بندی آنها** ۳
۲-۱ کارت هوشمند چیست؟ ۳
۲-۲ انواع کارت‌های هوشمند ۳
۲-۲-۱ کارت‌های مغناطیسی ۳
۲-۲-۲ کارت‌های دارای تراشه ۴
۲-۲-۳ کارت های غیر تماسی ۶

۳ **سلامت الکترونیک** ۷
۳-۱ تعریف ۷
۳-۲ اصلی ترین بنیان های مورد نیاز به منظور پیاده سازی نظام سلامت الکترونیک ۷
۳-۳ کاربردهای فناوری اطلاعات ۸
۳-۴ بررسی تطبیقی کشورهای منتخب سازمان بهداشت جهانی ۹

۴ **اجزا و عناصر سلامت الکترونیک** ۱۰
۴-۱ پرونده الکترونیکی سلامت ۱۰
۴-۲ انواع پرونده‌های الکترونیکی سلامت ۱۰
۴-۲-۱ پرونده الکترونیکی قابل اشتراک گذاری سلامت ۱۰
۴-۲-۲ پرونده الکترونیکی سلامت برای مراقبت یکپارچه ۱۰
۴-۲-۳ سایر پرونده های سلامت ۱۰
۴-۲-۴ پرونده الکترونیکی پزشکی ۱۱
۴-۲-۵ پرونده های الکترونیکی بیمار ۱۱
۴-۲-۶ پرونده مراقبتهای بهداشتی الکترونیکی ۱۱
۴-۲-۷ پرونده سلامت شخصی ۱۲
۴-۲-۸ پرونده پزشکی دیجیتال ۱۲
۴-۳ استانداردهای کدگذاری، طبقه بندی و اصلاح‌شناسی ۱۲
۴-۳-۱ MedDRA ۱۲
۴-۳-۲ ICD ۱۲
۴-۳-۳ CPT ۱۲
۴-۳-۴ LOINC ۱۳
۴-۴ استانداردهای مربوط به اسناد بالینی و پرونده الکترونیکی سلامت ۱۳
۴-۴-۱ CDISC ۱۳

۴-۴-۲ eCTD ۱۳
۴-۴-۳ CDA ۱۳
۴-۴-۴ CCD ۱۳
۴-۴-۵ HIMSS ۱۴
۴-۴-۶ ISO ۱۴
۴-۵ استانداردهای تبادل اطلاعات ۱۴
۴-۵-۱ HL7 . . . . . ۱۴
۴-۵-۲ EDI ۱۴
۴-۵-۳ DICOM ۱۵
۴-۵-۴ NCPDP ۱۵
۴-۵-۵ SPL ۱۵
۴-۶ استانداردهای برنامه های کاربردی ۱۵
۴-۶-۱ Med Corba ۱۵
۴-۶-۲ HIPAA ۱۶
۴-۶-۳ SSQS ۱۶

۵ پیاده سازی سامانه سلامت الکترونیک مبتنی بر کارت هوشمند ۱۷
۵-۱ معماری کارت هوشمند مورد استفاده ۱۷
۵-۱-۱ حافظه کاری ۱۷
۵-۱-۲ حافظه برنامه ۱۷
۵-۱-۳ حافظه کاربر ۱۸
۵-۲ ساختار حافظه کارت هوشمند ۱۹
۵-۳ سازوکارهای امنیتی ۱۹
۵-۳-۱ چالش ها ۲۰
۵-۳-۲ راهکارها ۲۰

۶ جمع‌بندی، نتیجه‌گیری و پیشنهادات ۲۳
۶-۱ جمع‌بندی و نتیجه‌گیری ۲۳
۶-۲ پیشنهادات ۲۳

منابع و مراجع ۲۴

فهرست اشکال و جداول

صفحه

شکل ۲-۱ یک نمونه رایج کارت مغناطیسی ۴
شکل ۲-۲ ارتباطات یک کارت دارای تراشه ۵

جدول ۳-۱بررسی سیاستهای ملی کشورهای منتخب سازمان بهداشت جهانی در خصوص
استفاده از فناوری اطلاعات و ارتباطات در نظام سلامت ۹

شکل ۵-۱ معماری تراشه به کار رفته در کارت هوشمند BULL CP8 . . . . . ۱۸
شکل ۵-۲ یک فرآیند رمزنگاری متقارن ۲۲
شکل ۵-۳ پیاده‌سازی الگوریتم DES در یک کارت هوشمند ۲۲

بخش اول

مقدمه

توسعه و پیشرفت فناوری اطلاعات و ارتباطات، کلیه علوم و فناوری های دیگر را دچار تحول و دگرگونی نموده و حتی سبک زندگی بشر را دستخوش تغییرات کرده است. حوزه بهداشت و درمان و نظام سلامت نیز از این تحول و دگرگونی تاثیر پذیرفته است. حوزه بهداشت و درمان ویژگی های متفاوتی نسبت به سایر حوزه های علم و فناوری کاربردی داشته و از حساسیت های ویژه ای برخوردار می باشد. برای بهبود کیفیت ارائه ی خدمات در این حوزه اقدامات متعددی در دنیا صورت گرفته که به کارگیری کارت های هوشمند سلامت یکی از جدیدترین و کاراترین دستاورد های دولت ها در حوزه ی سلامت در کشور های توسعه یافته می باشد [۱].

در حوزه بهداشت و درمان، با سلامت افراد و در نتیجه جامعه و حیات انسان ها سروکار داریم که از اهمیت و ضرورت ویژه ای در امنیت ملی و اجتماعی در جهان امروز برخوردار بوده و از شاخص های اصلی توسعه کشورها می باشد. همچنین کلیه خدمات و فرایندهای بهداشتی و درمانی بصورت فراسازمانی بوده و برخلاف سایر حوزه ها که مجموع فرایندها در یک سازمان انجام می شود، در حوزه بهداشت و درمان توسط چند دستگاه مستقل انجام می گردد؛ وزارت بهداشت، سازمان های بیمه، شرکت های بیمه تکمیلی مراکز و موسسات درمانی و درمانگران همگی در فرایند درمان شهروندان نقش داشته و هر یک متولی بخشی از سرویس ها و خدمات می باشند. این ویژگی ها موجب پیچیدگی و ایجاد چالش در روش ها و استانداردهای سلامت الکترونیکی گردیده است. معماری و طراحی سیستم هایی که هر بخش از فرآیند درمان را در یک سازمان مدیریت، پیگیری و کنترل می کنند از چالش های اصلی سلامت الکترونیکی در کشورها می باشد. از طرف دیگر افزایش تعداد نقش آفرینان در صحنه سلامت الکترونیکی بطور طبیعی موجبات گسترش بازار آن را نیز فراهم می نماید.

با توجه به دشوار بودن هماهنگی های بین سازمانی در کشورها، این ویژگی ها منجر به تشدید چالش‌های سلامت الکترونیکی می شوند. راه برون رفت و مقابله با نابسامانی های بخش بهداشت و درمان، رویکرد به سلامت الکترونیکی و ایجاد زیرساخت های الکترونیکی جهت تعامل های فراسازمانی و ارائه سرویس ها و کنترل فرآیند ها می باشد.

به علاوه، وجود گروه ها و مراکز متعدد پزشکی اعم از پزشک‌های متخصص، پزشک‌های عمومی، بیمارستان‌ها، درمانگاه‌ها و شرکت‌های بیمه‌کننده‌ی پزشکی گوناگون، به طور فزاینده ای کار مدیریت اطلاعات پزشکی بیماران را دشوارتر ساخته است که به ناچار باعث پایین آمدن کیفیت ارائه ی خدمات پزشکی مطلوب می‌گردد.

تکنولوژی کارت هوشمند الکترونیک در راستای بهبود بسیاری از ناگواری های یادشده می تواند برای ساده‌سازی مدیریت اطلاعات پزشکی و بهبود کیفیت ارائه ی خدمات پزشکی مورد استفاده قرار بگیرد

تا یک سامانه ی متمرکز نگهداری اطلاعات بیمار به طور الکترونیکی پیاده سازی شود. پیاده‌سازی این سامانه منجر به ایجاد چالش های امنیتی جدیدی نیز می‌شود و مهمترین آنها که شامل "صحت اطلاعات" و "محرمانگی اطلاعات" است، باید به نحوی در هر سامانه ای با هر نوع نحوه پیاده‌سازی بررسی و ارزیابی شوند [۲].

هدف اصلی این پروژه در نهایت ارائه یک نحوه پیاده‌سازی این سامانه ی سلامت مبتنی بر کارت هوشمند می باشد که جهت تحقق این هدف، ابتدا در فصل دوم مفاهیم کارت های هوشمند مورد بحث قرار می‌گیرند. در فصل سوم مفاهیم ضروری سلامت الکترونیک جهت تحقق هدف یادشده ارائه می‌شوند و در فصل چهارم با معرفی استانداردها و سایر عناصر به کار رفته در سلامت الکترونیک، موضوع روشن‌تر می‌گردد. در فصل پنجم مباحث مربوط به کارت هوشمند از فصل دوم و مباحث مربوط به سلامت الکترونیک از فصل های سوم و چهارم با هم ترکیب می‌شوند و معماری یک سامانه سلامت الکترونیک مبتنی بر کارت هوشمند ارائه می‌شود و معماری کارت به کاررفته در این سامانه، چالش های امنیتی و راهکارهای موجود به طور کامل مورد بحث قرار می‌گیرند تا هدف کلی پروژه تحقق بیابد. نهایتاً موارد گفته شده در فصل ششم جمع‌بندی می‌شوند و نتیجه گیری حاصل از این کار پژوهشی و پیشنهادات برای ادامه کار در این زمینه ارائه می‌شوند.

بخش دوم

شناخت کارت‌های هوشمند و دسته‌بندی آنها

۲-۱ کارت هوشمند چیست؟

کارت هوشمند، عبارت است از یک کارت پلی وینیل کلراید [۱] استاندارد که به یک پردازنده کوچک مجهز شده است. این مدل کارت دارای ریزپردازنده [۲] است که علاوه بر ذخیره‌سازی اطلاعات، قادر به پردازش داده‌های روی کارت نیز می‌باشد. در کنار ریز پردازنده در این کارت حافظه‌های ROM [۳] ، RAM [۴] ، EEPROM [۵] یا Flash-ROM و درگاه سریال نیز قرار دارد که سخت‌افزار مورد نیاز برای پردازش داده‌ها را فراهم می‌آورد[۲].

۲-۲ انواع کارت‌های هوشمند

کیث مایز [۳] در فصل اول کتاب خودش کارت های هوشمند را به صورت زیر دسته بندی می‌کند:

۲-۲-۱ کارت‌های مغناطیسی

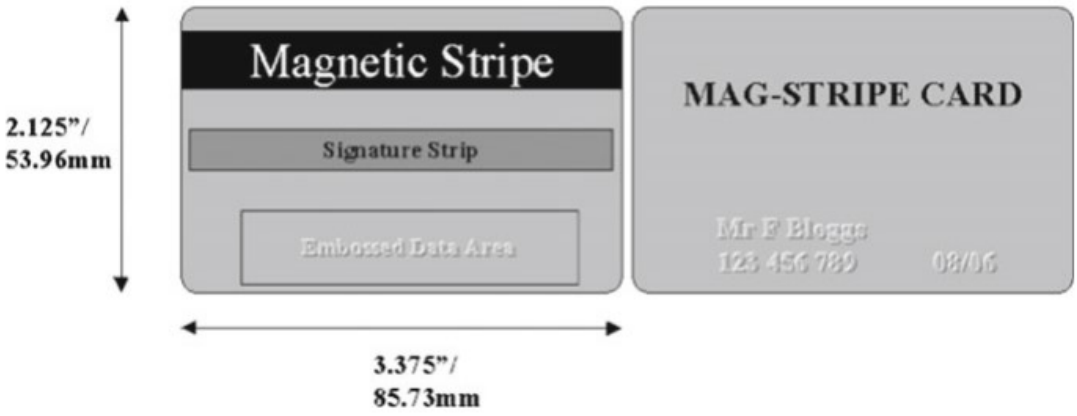
کارت‌های مغناطیسی [۶] از قدیمی‌ترین ابزارهای پرداخت الکترونیکی در دنیا به حساب می‌آیند و پیشینه آن‌ها در زمانی بسیار دور در استفاده از نوارهای فلزی برای ضبط صدا ریشه دارد.

اندکی پس از نوارهای ضبط صدا، ضبط مغناطیسی داده‌های دیجیتالی کامپیوتر روی نوار پلاستیکی حاوی اکسید آهن در سال ۱۹۵۰ ابداع شد و کارت‌های مغناطیسی به شکل امروزی در ۱۹۶۰ توسط IBM ساخته شدند. در بخش پشتی یک کارت مغناطیسی نوار تیره‌ای حاوی ذرات فلزی وجود دارد که با تغییر خاصیت مغناطیسی اطلاعات درون خود را دستخوش تغییر می‌کند. عرض این نوار تیره ۹.۵

[1] PVC
[2] Microprocessor
[3] Read Only Memory
[4] Random Access Memory
[5] Electrically Erasable Programmable Read Only Memory
[6] Magnetic Stripe Cards

میلیمتر است و نزدیک به ۵.۶ میلیمتر از لبه پایینی کارت فاصله دارد. در این نوار تیره سه مسیر [۷] وجود داشته که هرکدام نزدیک به ۲.۸ میلیمتر قطر دارند.

یک نمونه متداول کارت مغناطیسی در شکل ۲-۱ نشان داده شده است.



شکل ۲-۱: یک نمونه رایج کارت مغناطیسی

۲-۲-۲ کارت‌های دارای تراشه

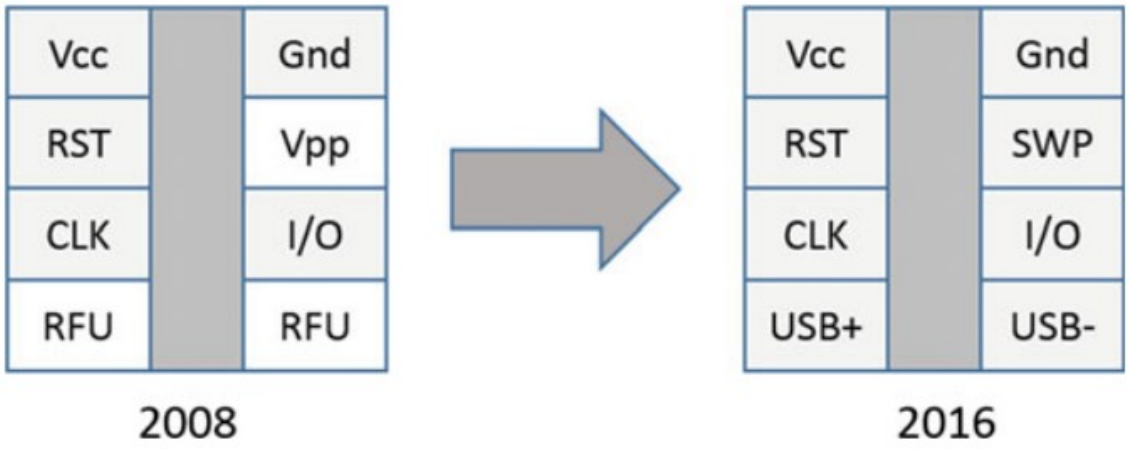
کارت هوشمند دارای تراشه [۸] کارتی است که بر روی آن یا در بین لایه‌های آن یک تراشه سیلیکونی کوچک نصب گردیده؛ این تراشه شامل ریزپردازنده جهت پردازش و حافظه جهت ذخیره اطلاعات می باشد. عملیات خواندن و نوشتن اطلاعات بر روی کارت به کمک ریزپردازنده و از طریق سیستم عامل کارت انجام می شود. این ریزپردازنده معمولا در زیر یک اتصال طلایی در یک طرف کارت قرار دارد. این ریزپردازنده در کارتهای هوشمند در حقیقت جایگزین نوارمغناطیسی در کارتهای مغناطیسی شده است. کارتهای هوشمند میتوانند خیلی بیشتر از یک کارت مغناطیسی داده ذخیره کنند و با ذخیره الگوریتم های رمزنگاری، امنیت تبادلات را بهبود بخشند. این تراشه نیمه هادی می تواند همچون یک حافظه و یا یک پردازنده عمل کند.

ارتباطات یک کارت دارای تراشه در شکل ۲-۲ نشان داده شده است.

- **کارت‌های حافظه مستقیم**

این کارت‌ها فقط داده‌ها را ذخیره می‌کنند و هیچ قابلیت پردازش اطلاعاتی ندارند. کارت‌های حافظه مستقیم اغلب با نیمه‌هادی های I2C [۹] یا نیمه رسانا های فلزی سریالی ساخته می‌شوند. این نوع از کارت‌ها به طور سنتی کمترین هزینه در هر بیت را برای کاربر ایجاد می‌کنند. در حال حاضر این نوع از کارت‌های هوشمند با کمک تعداد زیادی از ریزپردازنده‌ها برای بازار GSM [۱۰]

[7] Track
[8] Chip Card
[9] Inter-Integrated Circuit
[10] Global System for Mobile Communications



شکل ۲-۲: ارتباطات یک کارت دارای تراشه

تغییر کرده‌اند. این تغییرات باعث شده است که مزایای چشمگیری به کارت حافظه مستقیم اضافه شود و قدرت عملکرد آنها را بالا ببرد. درواقع می‌توان کارت‌های حافظه مستقیم را به‌عنوان یک نوع فلاپی دیسک در نظر گرفت که اطلاعات را مستقیماً ذخیره می‌کنند. لازم به ذکر است که این نوع از کارت‌های هوشمند توانایی عرضه اطلاعات خود به سیستم خواننده را ندارند و باید با استفاده از سیستم میزبان خوانده شوند. کارت حافظه مستقیم به راحتی رونوشت می‌شود و با شیوه های متداول شناسایی کارت قابل ردیابی نیست.

- **کارت‌های حافظه محافظت شده**

این کارت دارای ورودی کنترل شده برای کنترل دسترسی به حافظه کارت است. در برخی موارد از این نوع کارت به‌عنوان کارت حافظه هوشمند نیز یاد می‌شود، زیرا می‌تواند از اطلاعات ذخیره شده حفاظت کند و ترتیبات امنیتی خوبی دارد. ساختار کارت حافظه محافظت شده به صورتی است که می‌توان بخشی از آن را به خواندن و بخشی از آن را به درج اطلاعات اختصاص داد. سیستم امنیتی این نوع از کارت‌های هوشمند به کمک رمز عبور اجرایی می‌شود و بخش‌های مختلف آن امکان استفاده از آنها به‌عنوان کارت‌های چندمنظوره را فراهم آورده است. کارت حافظه محافظت شده به آسانی رونوشت نمی شود اما امکان هک شدن آن وجود دارد. می‌توان از این کارت به عنوان کارت شناسایی استفاده کرد.

- **کارت های حافظه یکبار مصرف**

کارت‌های حافظه یکبار مصرف نوع خاصی از کارت‌های حافظه هستند که به ذخیره‌سازی مقدار خاصی از اطلاعات اختصاص یافته‌اند و زمانی که این حافظه مورد استفاده قرار گیرد، امکان استفاده مجدد ندارد. درواقع فضای داخلی این نوع از کارت‌های هوشمند به چندین بخش تقسیم می‌شود و کاربر می‌تواند اطلاعات خود را به هر بخش وارد کند. بهترین مثال برای این نوع از کارت‌های هوشمند، کارت‌های تلفن هستند که تراشه آنها به ۱۲ تا ۶۰ سلول مستقل تقسیم شده است. در

هربار استفاده یکی از سلول‌های این کارت حافظه مصرف می‌شود و درنهایت پس از مصرف کلیه سلول‌ها باید دور انداخته شود.

- **کارت‌های دارای ریزپردازنده**

این نوع کارت‌ها در مقایسه با کارت‌های مغناطیسی دارای حجم حافظه بالاتر و امنیت داده‌های بهتر می‌باشند. این کارت‌ها معمولاً دارای پردازنده‌های ۸ بیتی، همراه با ۱۶ کیلوبایت حافظه فقط خواندنی و ۵۱۲ بایت حافظه از نوع RAM می‌باشند. ازجمله کاربردهای کارت‌های فوق که رمزنگاری بصورت درونی [11] روی کارت تعبیه شده است عبارتند از: کارت های بانکی، کارت‌های دسترسی به شبکه های امن، کارت های محافظ تلفن همراه برای جلوگیری از دسترسی های غیرمجاز و کارت هایی که در گیرنده های تلویزیون جهت کنترل دسترسی به کانال ها مورد استفاده قرار می‌گیرند.

۲-۲-۳ کارت های غیر تماسی

کارت هوشمند غیر تماسی یک نوع خاص از کارت‌های هوشمند هستند که از شناسایی رادیویی [12] بین کارت و دستگاه کارت‌خوان استفاده می‌کنند. تمامی این مراحل بدون جابجایی کارت صورت می‌گیرد و نیازی به تماس کارت با دستگاه کارتخوان ندارند. کارت‌های RFID به انواع مختلفی تقسیم می‌شوند که برخی از آنها با فرکانس ۱۲۵ مگاهرتز کار می‌کنند و برخی دیگر مانند کارت‌های UHF [13] با فرکانس ۸۶۰ تا ۹۶۰ مگاهرتز عمل می‌کنند.

اولین نمونه از کارت‌های غیر تماسی برای استفاده سریع و آسان از پرداخت کرایه مورد استفاده قرار گرفتند که به دلیل پایین بودن امنیت، چندان موردتوجه قرار نگرفتند. این کارت‌ها در فرکانس ۵۶.۱۳ مگاهرتز کار می‌کنند و مطابق با استاندارد ISO 14443 هستند. حافظه استفاده شده درکارت‌های غیر تماسی به صورت محافظت شده بوده و برای پرداخت‌های مالی و خرده‌فروشی محبوبیت بالایی دارند. با وجود اینکه کارت‌های هوشمند غیر تماسی از امتیازات مهمی برخوردارند، اما عملیات رمزنگاری محدود و فاصله محدود بین کارت و دستگاه کارت‌خوان باعث شده است که فراگیری آنها کمتر از میزان تصور باشد.

[11] Built-in

[12] Radio-Frequency Identification (RFID)

[13] Ultra High Frequency

بخش سوم

سلامت الکترونیک

۳-۱ تعریف

سلامت الکترونیکی [1] به معنی استفاده از اطلاعات، رایانه ها و ارتباطات از راه دور برای پشتیبانی از نیازهای بیماران و ارتقاء سلامت شهروندان است. هدف آن پشتیبانی از ارتقاء سلامت شهروندان، افزایش کیفیت سطح مراقبت های بهداشت و درمان، بهینه سازی هزینه های درمان، و هدایت هزینه های درمان به سمت پیشگیری است. سلامت الکترونیکی استفاده از توانمندی های اطلاعات الکترونیکی برای اطمینان از ارائه مراقبت های صحیح درمانی است. بنابراین سلامت الکترونیکی در مورد تبدیل روش های سنتی به روش های نوین و فناوری های بکار برده شده صحبت می کند [۴].

تعریف سازمان بهداشت جهانی از سلامت الکترونیکی عبارت است از: استفاده از فناوری اطلاعات و ارتباطات در حوزه سلامت جهت نگهداری، انتقال و استفاده از داده های دیجیتالی در حوزه سلامت در کاربردهای درمانی، آموزشی و اداری از طریق شبکه محلی یا راه دور را سلامت الکترونیکی می نامند.

۳-۲ اصلی ترین بنیان های مورد نیاز به منظور پیاده سازی نظام سلامت الکترونیک

طبق بررسی ها اصلی ترین بنیان های مورد نیاز برای پیاده سازی نظام سلامت الکترونیک عبارتند از [۵]:

۱. ایجاد و تقویت انگیزه در ارائه دهندگان خدمات سلامت الکترونیک از طریق در نظر گرفتن برخی مشوق‌های خاص در این زمینه.

۲. تدوین استانداردهای مورد نیاز سیستم سلامت الکترونیک

۳. حفظ ایمنی و محرمانگی اطلاعات سلامت

۴. سرمایه گذاری مناسب و برنامه ریزی در حوزه سلامت الکترونیک

[1] eHealth

۳-۳ کاربردهای فناوری اطلاعات

در نتیجه توسعه فناوری‌های ارتباطی و اطلاعاتی، در نظام های اجتماعی تحولاتی به وجود آمده است. حوزه خدمات درمانی و بهداشتی نیز تحت تاثیر این فناوری‌ها به نظام های جدید ارائه خدمات دست پیدا کرده است که عبارتند از:

- **نظام ارائه خدمات پزشکی بین مراکز پزشکی**

وجود تجهیزات جدید الکترونیکی در حوزه تشخیص و درمان، ارتباط بین مراکز ارائه خدمات را امکان پذیر کرده است. مواردی چون پزشکی از راه دور و زیر مجموعه های آن چون عکس برداری از راه دور، چشم پزشکی از راه دور، پوست شناسی از راه دور، بررسی قلب از راه دور و انجام جراحی‌های پزشکی تحت نظارت کارشناسان از سرتاسر دنیا از جمله خدمات این نظام در حوزه بهداشت و درمان در عصر اطلاعات است.

- **نظام ارائه خدمات پزشکی خارج از مراکز پزشکی**

مواردی چون مراقبت در خانه، مراقبت از راه دور و پایش از راه دور زیر مجموعه ای از کارهای قابل انجام در نظام خدمات نوین می باشند. بررسی وضعیت بیماران از راه دور در محل زندگی آن‌ها تاثیرات مثبتی را هم در مرحله تشخیص و هم در مرحله درمان بیماران به جا گذاشته است. کاهش هزینه های نگهداری بیمار، راحتی و آسایش بیمار، بررسی وضعیت بیمار در شرایط واقعی از زندگی روزمره، ثبت اطلاعات درمانی، ارتباط پیوسته با یک مرکز خدمات درمانی در هر موقعیت جغرافیایی، شبکه ارائه خدمات درمانی جهانی، و استفاده از بهترین پتانسیل های موجود در ارائه خدمات بهداشتی و درمانی، نمونه هایی از ویژگی های نظام سلامت الکترونیک می باشد. لازم به ذکر است که کاهش نیاز به ملاقات حضوری بین پزشک و بیمار به معنای نفی اهمیت معاینه بالینی و شرح‌حال بیمار نبوده و این دو پایه اصلی علم پزشکی، مقام اصلی خود را در علم پزشکی حفظ خواهند کرد.

- **نظام مدیریت سلامت الکترونیک در حوزه بهداشت عمومی**

ثبت اطلاعات بهداشتی و ایجاد شبکه جمع آوری اطلاعات بهداشتی بروز و امکان پردازش این اطلاعات و استفاده از نرم افزار های هوشمند، تصمیم سازی و تصمیم گیری در حوزه مدیریت بهداشت را بهبود خواهد بخشید و در راستای تحقق شعار "پیشگیری بهتر از درمان" حرکت خواهد کرد.

- **نظام مشاوره و آموزش از راه دور**

ابزار های چند رسانه ای بستر مناسبی جهت اجرای طرح آموزش مستمر در مناطق مختلف کشورها است. در راستای گسترش فرهنگ متخصص محوری و مشاوره در زندگی شخصی و اجتماعی افراد، به خصوص در حوزه بهداشت، انواع ابزارهای ارتباطی چندرسانه‌ای با ویژگی های متنوع و امکان

دسترسی در هر مکانی از کره زمین، کمک قابل توجهی در ایجاد ارتباطات موثر خواهند کرد. همچنین با پیاده سازی این نظام، شهروندان در سراسر دنیا می توانند از کلیه اطلاعات روزآمد سلامت آگاه شوند و در کنترل بیماری‌های خود و مراقبت های فردی موفق تر از گذشته عمل کنند.

۳-۴ بررسی تطبیقی کشورهای منتخب سازمان بهداشت جهانی

بر اساس سرشماری که در این خصوص سازمان بهداشت جهانی انجام داده است کشورهای کانادا، اتریش، هند، کره و آلمان از نظر وجود یا عدم وجود سیاست های ملی برای به کارگیری فناوری اطلاعات و ارتباطات [۲] در حوزه سلامت مورد بررسی قرار گرفته اند که نتایج آن در جدول ۳-۱ قابل مشاهده است [۶].

جدول ۳-۱: بررسی سیاستهای ملی کشورهای منتخب سازمان بهداشت جهانی در خصوص استفاده از فناوری اطلاعات و ارتباطات در نظام سلامت

کشور	شاخص های منتخب مرتبط با ICT								
	دسته بندی بانک جهانی	شاخص انتشار ICT(۲۰۰۲)	کاربری اینترنت به ازای هر نفر(۲۰۰۴)	میزان سواد در بزرگسالان(۲۰۰۴)	سیاست اطلاعات ملی	سیاست الکترونیکی ملی	سیاست ملی سلامت الکترونیکی	سیاست استانداردها	سیاست حفاظت شهروندان	سیاست تساوی
کانادا	۱	۰.۶۲۱۶	۶۲.۳۶	غیره	*	*	*	*	*	*
هند	۴	۰.۲۰۸۱	۳.۲۴	۶۱	*	*	*	*	*	*
اتریش	۱	۰.۵۶۹۹	۴۷.۵۲	غیره	*	*	*	*	*	*
آلمان	۱	۰.۶۱۱۴	۴۲.۶۷	غیره	*	*	*	*	*	*
جمهوری کره	۱	۰.۶۱۶۰	۶۵.۶۸	غیره	*	*	*	*	*	-

* این علامت نشان دهنده مثبت بودن سیاست مذکور در جدول فوق می باشد.

[2] Information and communications technology (ICT)

بخش چهارم

اجزا و عناصر سلامت الکترونیک

مهمترین اجزا، عناصر و استانداردهای به کار رفته در سلامت الکترونیک عبارتند از [۴، ۵]:

۴-۱ پرونده الکترونیکی سلامت

پرونده سلامت الکترونیکی [۱] در واقع مخزنی از اطلاعات مربوط به سلامت است که قابل پردازش با رایانه است و شامل بخش های مختلفی می باشد که در ادامه آنها را شرح می‌دهیم.

۴-۲ انواع پرونده‌های الکترونیکی سلامت

۴-۲-۱ پرونده الکترونیکی قابل اشتراک گذاری سلامت

پرونده الکترونیکی قابل اشتراک گذاری [۲] یک EHR است با یک مدل اطلاعاتی استاندارد شده که از سیستم های EHR مستقل می باشد و به طور ایمن ذخیره و منتقل می گردد و توسط کاربران مجاز با استفاده از برنامه های مختلف قابل دستیابی می باشد.

۴-۲-۲ پرونده الکترونیکی سلامت برای مراقبت یکپارچه

پرونده الکترونیکی سلامت برای مراقبت یکپارچه [۳] یک SEHR است که هدف اولیه آن پشتیبانی از مراقبت‌های مداوم، موثر و از لحاظ کیفی یکپارچه می باشد. ICEHR حاوی اطلاعات مربوط به گذشته، مربوط به حال و مربوط به آینده می باشد.

۴-۲-۳ سایر پرونده های سلامت

تقسیم بندی های مختلفی برای پرونده سلامت الکترونیکی قابل تعریف می باشد که برخی از آنها توسط استانداردها و موسسات تعریف شده اند که استفاده از آنها در کشورها و بخشهای بهداشت مختلف، غیر

[1] Electronic Health Record (EHR)

[2] Shared Electronic Health Record (SEHR)

[3] Integrated Care Electronic Health Record (ICEHR)

همسان بوده است.

۴-۲-۴ پرونده الکترونیکی پزشکی

پرونده الکترونیکی پزشکی [۴] را می توان به عنوان یک نمونه خاص EHR در نظر گرفت که محدود به حوزه پزشکی می باشد. این تعریف در آمریکای شمالی و تعدادی از کشورها از جمله ژاپن استفاده می شود. موسسه سیستم های اطلاعاتی مراقبتهای بهداشتی ژاپن [۵] یک سلسله مراتب پنج سطحی برای EMR تعریف کرده است [۴]:

- **EMR دپارتمانی:** حاوی اطلاعات پزشکی بیمار می باشد که توسط یک دپارتمان بیمارستانی واحد ارائه می شود (مانند پاتولوژی، رادیولوژی، داروخانه).
- **EMR بین دپارتمانی:** محتوی اطلاعات پزشکی بیمار از دو یا چند دپارتمان بیمارستان می باشد.
- **EMR بیمارستانی:** محتوی تمام یا بخش اعظمی از اطلاعات بالینی یک بیمارستان خاص می باشد.
- **EMR بین بیمارستانی:** محتوی اطلاعات پزشکی یک بیمار از دو یا چند بیمارستان می باشد.
- **پرونده مراقبتهای بهداشتی الکترونیکی:** مجموعه ای از اطلاعات سلامت فردی از تمام منابع می باشد.

۵-۲-۴ پرونده های الکترونیکی بیمار

خدمات ملی سلامت انگلستان [۶]، پرونده الکترونیکی بیمار [۷] را شامل "اطلاعات مراقبتی بهداشتی یک فرد به صورت دوره ای که توسط یک موسسه انجام می گیرد." تعریف می نماید. NHS تاکید می کند که پرونده الکترونیکی بیمار با مراقبت هایی که بیمارستان ها یا واحدهای تخصصی بصورت کوتاه مدت ارائه می کنند، در ارتباط می باشد.

۶-۲-۴ پرونده مراقبتهای بهداشتی الکترونیکی

پرونده مراقبت های بهداشتی الکترونیکی [۸] شامل استاندارد CEN13606 (انفورماتیک سلامت: ارتباطات پرونده مراقبتهای بهداشتی الکترونیکی) می باشد. می توان از آن به عنوان مترادف EHR نام برد که EHR امروزه در اروپا به سرعت جایگزین EHCR می شود.

[4] Electronic Medical Record (EMR)
[5] Japanese Association of Healthcare Information Systems (JAHIS)
[6] National Health Service (NHS)
[7] Electronic Patient Record (EPR)
[8] Electronic Health-Care Record (EHCR)

۴-۲-۷ پرونده سلامت شخصی

مشخصه کلیدی پرونده سلامت شخصی [۹] این است که تحت کنترل صاحب پرونده می باشد که شامل اطلاعات از پیش تعریف شده یا اطلاعات وارد شده توسط فرد می باشد.

۴-۲-۸ پرونده پزشکی دیجیتال

پرونده پزشکی دیجیتال [۱۰] یک پرونده تحت وب است که می تواند کارایی EMR، EPR یا EHR را داشته باشد.

۴-۳ استانداردهای کدگذاری، طبقه بندی و اصلاح‌شناسی

۴-۳-۱ MedDRA

MedDRA [۱۱] دیکشنری پزشکی برای فعالیتهای هماهنگ کننده و یک ترمینولوژی حایز اهمیت بالینی است که توسط مراکز هماهنگ کننده، صنعت بیوفارماکوتیک و صنعت محصولات پزشکی، از فعالیتهای پیش از فروش تا بعد از آن، برای ورود داده ها، بازخوانی، ارزیابی و ارایه آنها استفاده می شود.

۴-۳-۲ ICD

طبقه بندی بین المللی بیماریها [۱۲] در ایالات متحده به منظور تهیه راهی برای طبقه بندی اطلاعات موربیدیتی برای فهرست کردن پرونده های پزشکی، بازخوانی موارد پزشکی و برنامه های سیار و سایر برنامه های سلامت و همچنین آمار گیری پایه پزشکی بوجود آمد.

۴-۳-۳ CPT

CPT [۱۳] توسط موسسه طبی آمریکا در سال ۱۹۶۶ ایجاد شده است. از این کدها برای صدور صورتحساب فرآیندهای پزشکی استفاده می شود. هر سال یک سالنامه تهیه می شود که تغییرات مرتبط با بروز رسانی های قابل توجه در عرصه اصطلاح‌شناسی و کار عملی را شامل می گردد. نسخه اخیر آن حاوی بیش از ۸ هزار کد و تعریف می باشد.

[9] Personal Health Record (PHR)
[10] Digital Medical Record (DMR)
[11] Medical Dictionary for Regulatory Activities
[12] The International Classification of Diseases
[13] Current Procedural Terminology

LOINC ۴-۳-۴

LOINC [۱۴] یک بانک اطلاعاتی و استاندارد جهانی برای تعریف مشاهدات بالینی و خدمات آزمایشگاهی می باشد.

۴-۴ استانداردهای مربوط به اسناد بالینی و پرونده الکترونیکی سلامت

CDISC ۱-۴-۴

کنسرسیوم استانداردهای تبادل داده های بالینی [۱۵] ، موسسه ای است که ماموریتش ایجاد و پشتیبانی از استانداردهای جهانی مستقل از پایگاه است که سیستم های اطلاعاتی را قادر می سازد پژوهش های پزشکی را بهبود بخشیده و بخش های مراقبت های بهداشتی را به هم مرتبط می سازد.

eCTD ۲-۴-۴

eCTD [۱۶] به عنوان یک سازمان صنعتی برای انتقال اطلاعات تنظیم کننده میان بنگاه ها و به طور همزمان، تسهیل ایجاد، بازخوانی، مدیریت و بایگانی ارایه های الکترونیکی می باشد. تمرکز آن بر ارایه قابلیت انتقال برنامه های ثبت به طور الکترونیکی می باشد.

CDA ۳-۴-۴

CDA [۱۷] یک استاندارد مبتنی بر XML برای کدکردن، ساختاربندی و ارایه اسناد بالینی قابل تبادل می باشد.

CCD ۴-۴-۴

CCD [۱۸] یک استاندارد فعال در پاسخ به نیاز سازماندهی با قابلیت انتقال اطلاعات مربوط به بیمار است.

[14] Logical Observation Identifiers Names and Codes
[15] Clinical Data Interchange Standards Consortium
[16] Electronic Common Technical Document
[17] Clinical Document Architecture
[18] Continuity of Care Document

HIMSS ۵-۴-۴

سیستم های مدیریتی و اطلاعاتی مراقبت های بهداشتی [۱۹] یک موسسه سلامت است که عمدتا بر ارایه راهبردهای استفاده بهینه از انفورماتیک پزشکی و سیستم های مدیریتی استوار است.

ISO ۶-۴-۴

استاندارد ایزو [۲۰] شامل مجموعه استانداردهای حوزه مختلف می باشد که بخش TC215 آن شامل استانداردهای داده ورزی اطلاعات سلامت می باشد. استاندارد های مربوط به ارتباط تجهیزات پزشکی، ارتباط پرونده های الکترونیکی سلامت، خدمات گواهی نامه های دیجیتال و مدیریت سیاست های آن، تبادل اطلاعات میان سامانه های سلامت الکترونیکی مختلف، لغت‌نامه سیستم های اصطلاح‌شناسی، استانداردهای مربوط به کارت سلامت (از جمله: ویژگی های کلی، سیستم های شماره گذاری و روش های ثبت و غیره)، انواع اطلاعات مربوط به بیمار، از شناسایی گرفته تا تجویز دارو، استفاده از تکنولوژی بدون سیم و موبایل، گزارش دهی عوارض داروها، پرونده دارویی بیماران، مدیریت امنیت و بسیاری از موارد دیگر بخشی از استانداردهای مقرر شده توسط ISO هستند.

۵-۴ استانداردهای تبادل اطلاعات

HL7 ۱-۵-۴

HL7 [۲۱] استانداردی برای تعامل داده های بالینی در اکثر موسسات می باشد. اعضای HL7 دست اندرکار تهیه یک ساختار (و استانداردهای مربوطه) برای تبادل، یکپارچه سازی، به اشتراک گذاشتن و بازخوانی اطلاعات الکترونیکی مربوط به سلامت می باشند و تعریف می کنند که چگونه اطلاعات بسته بندی و فرستاده می شوند.

EDI ۲-۵-۴

EDI [۲۲] عبارت است از تبادل داده ها از کامپیوتری به کامپیوتر دیگر با استفاده از استاندارد پیغام رسانی به طوری که حداقل دخالت انسانی در کار باشد. درواقع EDI عبارت است از راهکارهای خاص مورد توافق برای تبادل اطلاعات و انتقال آن با یک برنامه کاربردی خاص. با وجود اینکه EDI امروزه در فناوری

[19] Health Information Management Systems Society

[20] International Organization for Standardization

[21] Health Level 7

[22] Electronic data interchange

هایی مانند XML و اینترنت کاربردی ندارد، هنوز ساختار داده هایی که توسط تعداد زیادی از برنامه ها استفاده می گردد از نوع همین EDI می باشد.

DICOM ۳-۵-۴

DICOM [۲۳] به منظور انتقال تصاویر ایجاد شده است و به طور بین المللی برای بایگانی تصاویر و سیستم های ارتباطی (PACS) مورد استفاده قرار می گیرد. این استاندارد توسط کمیته مشترک کالج رادیولوژی ایالات متحده (ACR) و موسسه کارخانه‌های الکترونیکی ملی (NEMA) تهیه شده است تا نیازهای کارخانه ها و کاربران دستگاه های تصویربرداری پزشکی را برای ارتباط دستگاه ها در شبکه های استاندارد برآورده سازد.

NCPDP ۴-۵-۴

تمرکز NCPDP [۲۴] بر ارایه پیغامهای مربوط به تجویز دارو است و برای ایجاد و پیشبرد تبادل داده ها و پردازش استانداردها برای بخش خدمات داروخانه کار می کند.

SPL ۵-۵-۴

استفاده از SPL [۲۵] به درخواست اداره ی کل خوراک و داروی آمریکا برای ارائه استانداردی جهت برچسب زنی محصولات دارویی بر اساس استاندارد دیگر HL7 بوده و امروزه به عنوان سازوکاری برای تبادل اطلاعات درمانی استفاده می شود.

۶-۴ استانداردهای برنامه های کاربردی

Med Corba ۱-۶-۴

استانداردی صنعتی برای تعامل شیءگرا میان سیستمهای کامپیوتری مجزا در زمینه سلامت جهت اعتلای کیفیت مراقبتها و کاهش هزینه ها با استفاده از فناوریهای CORBA در محیطهای مختلف مراقبتهای بهداشتی می باشد. رویکرد آن شامل سطوح متعدد خدمات/بخشی، سطح سازمانی، سطح موسسه و غیره می باشد.

[23] Digital Imaging and Communications in Medicine

[24] National Council for Prescription Drug Programs

[25] Structured Product Labeling

HIPAA ۲-۶-۴

قانون انتقال و پاسخگویی الکترونیک بیمه سلامت [۲۶] در سال ۱۹۹۶ توسط کنگره ایالات متحده جهت پوشش بیمه برای کارکنان و خانواده هایشان برای مواقعی که شغلشان را از دست می دهند یا عوض می‌کنند تصویب شد. دومین قسمت HIPAA که مقررات تسهیل اداری می باشد، نیازمند ایجاد استانداردهای ملی برای نقل و انتقالات مراقبتهای بهداشتی الکترونیکی و شناسه های ملی می باشد. مقررات مذکور همچنین امنیت سیستم را نیز شامل می گردد. هدف غایی آن "بهبود تاثیر سیستمهای ملی سلامت با تشویق به استفاده گسترده از تبادل اطلاعات بین کامپیوترها و استفاده از استانداردهای مورد قبول در سیستم سلامت ایالات متحده" می باشد.

SSQS ۳-۶-۴

استانداردهای شایستگی مدرسه هوشمند [۲۷] شامل استانداردهای کیفیت نرم افزارهای مرتبط با امنیت برای مراقبت های بهداشتی می باشد که تحت نام اختصاری UNE-CR 13694 نیز شناخته می شود و چند شاخصه کیفیت را که در ارتباط با امنیت و حفاظت در نرم افزار سلامت الکترونیکی است، پیشنهاد می کند.

[26] Health Insurance Portability and Accountability Act

[27] Smart School Qualification Standards

بخش پنجم

پیاده سازی سامانه سلامت الکترونیک مبتنی بر کارت هوشمند

در این فصل قرار است تا از آموخته های فصل های گذشته بهره بگیریم و با کنار هم قرار دادن مطالب گفته شده در مورد کارت های هوشمند و سلامت الکترونیک، به شرح پیاده سازی یک سامانه سلامت الکترونیک مبتنی بر کارت هوشمندی که معماری آن بیان می‌شود بپردازیم، چالش های موجود برای تحقق این هدف را بیان کنیم، و نهایتاً راه حل های ممکن برای حل آنها را نیز تشریح کنیم.

۵-۱ معماری کارت هوشمند مورد استفاده

از آنجایی که کارت های مغناطیسی که در بخش دوم این پژوهش آنها را معرفی کردیم، امنیت بسیار پایینی دارند، برای پیاده سازی این سامانه اصلاً مناسب نیستند؛ در نتیجه باید به سراغ کارت های "هوشمند" برویم و برای این بخش، کارت ۳.۰۷۲ بایتی BULL CP8 را انتخاب می‌کنیم. این کارت با وجود جدید نبودن فناوری به کارت رفته در تولیدش، هنوز هم مورد استفاده قرار می‌گیرد و به سبب ویژگی‌های عامی که دارد و وجود این ویژگی‌ها در تقریباً همه‌ی کارت های هوشمند امروزی، کارت بسیار مناسبی برای توضیح چالش ها و نحوه ی برطرف کردن مشکلات امنیتی است. ریزپردازنده به کار رفته در این کارت با سه نوع حافظه در تعامل است. در شکل ۵-۱ معماری تراشه‌ی این کارت نمایش داده شده است که در ادامه به توضیح قسمت های مختلف حافظه ی آن می‌پردازیم [۲]:

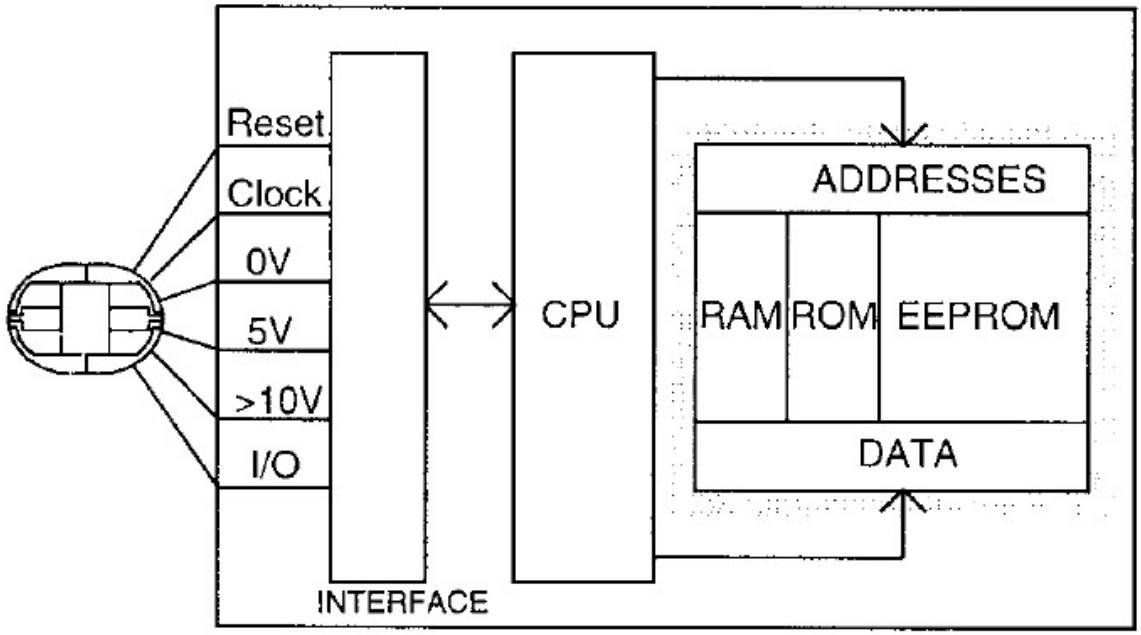
۵-۱-۱ حافظه کاری

از نوع RAM می‌باشد که با خاموش شدن، اطلاعات روی آن از دست می‌رود.

۵-۱-۲ حافظه برنامه

از نوع ROM می‌باشد که با روشن و خاموش شدن اطلاعات روی آن از بین نمی‌رود. "سیستم عامل" در این حافظه قرار داده می‌شود که وجود آن برای رسیدن به "هوشمندی" در سامانه ضروری است.

ویزگی های اصلی سیستم عامل کارت هوشمند عبارتند از:



شکل ۵-۱: معماری تراشه به کار رفته در کارت هوشمند BULL CP8

- **سرویس** برای ارتباط با دنیای بیرون و انجام عملیات های کاربر
- **اطمینان از امنیت** اطلاعات نگهداری شده روی کارت
- **پیاده سازی الگوریتم های رمزنگاری** برای بالا بردن سطح امنیت اطلاعات

۵-۱-۳ حافظه کاربر

این حافظه از نوع EEPROM می‌باشد و پس از ساخت کارت، خالی است. حافظه کاربر به چهار فضا تقسیم شده است:

- **فضای نهان:** ویژگی قسمت نهان این است که تنها یکبار می‌تواند نوشته شود و غیر قابل خواندن است. ساختار یکپارچه [۱] دارد و ویژگی های خاصی در آن برای حفاظت از دو اصل تمامیت اطلاعات [۲] و محرمانگی اطلاعات [۳] تعبیه شده اند که از جمله آنها می‌توان به قرار گرفتن انواع کدهای مخفی برای رمزنگاری، که برای هر کارت منحصر به فرد هستند، اشاره کرد. پردازنده اجازه ی خواندن از این قسمت را به هیچ عامل بیرونی نمی‌دهد.
- **فضای دسترسی:** این قسمت از حافظه کاربر تعداد دفعات درخواست با رمز درست یا غلط را ذخیره می‌کند تا جلوی کلاهبرداری را بگیرد.

[1] Monolithic
[2] Data Integrity
[3] Data Confidentiality

- **فضای عمومی:** بدون کلید (رمز) اجازه ی دسترسی به این قسمت داده می‌شود و برای نگهداری اطلاعات غیر محرمانه به کار گرفته می‌شود.
- **فضای کاری:** هدف این قسمت، کنترل جریان داده در تمام طول دوره ی فعالیت کارت است و از دید برنامه مهمترین قسمت در بین این چهار قسمت می‌باشد.

۵-۲ ساختار حافظه کارت هوشمند

همانطور که قبلتر اشاره کردیم، کارت هوشمند به کار رفته حافظه‌ی بسیار محدودی (در حد ۳ کیلوبایت) را داراست و در این ظرفیت پایین، نگهداری اطلاعات خیلی زیاد بدون ساختار مشخص، غیرممکن است. از طرفی اطلاعات بیمار ممکن است خیلی حیاتی باشد و ضروری است تا ساختاری را ارائه دهیم تا بتوان تمام اطلاعات مورد نیاز هر بیمار را در همین حافظه‌ی محدود نگهداری کرد.

برای این منظور، می‌دانیم که خیلی از قسمت های "سوابق بیمار" تنها نیاز به یک پاسخ "آری" یا "نه" دارند؛ یعنی مثلاً بیمار یا سابقه‌ی ناراحتی قلبی در گذشته داشته و یا نه. از همین نکته کمک می‌گیریم و برای هر "سابقه بیماری"، تنها یک بیت مشخص را در نظر می‌گیریم که یک بودن آن به معنی داشتن این سابقه بیماری و صفر بودن آن به معنی نداشتنش می‌باشد. با همین تکنیک در تنها ۳۲ بایت که شامل ۲۵۶ بیت است، سابقه ۲۵۶ نوع بیماری ضروری را نگهداری می‌کنیم که کاملاً نیاز مورد نظر را برطرف می‌کند.

برای بهبود بیشتر استفاده از حافظه، به هر پزشک یک شناسه منحصر به فرد اختصاص می‌دهیم تا فضای زیادی از کارت برای نگهداری اطلاعات پزشکی که بیمار را ویزیت کرده هدر نرود. بنابراین هر یادداشت مربوط به ویزیت بیمار که در کارت ذخیره می‌شود، تنها شامل شناسه پزشک، تاریخ ویزیت، و یک رونوشت از "سوابق بیماری" فرد می‌باشد.

با تکنیک‌های گفته شده می‌توان تا پنجاه ویزیت را تضمین کرد که در کارت هوشمند نگهداری شوند. هر کارت هوشمند اطلاعات تا این میزان ویزیت پزشک را نگه می‌دارد و پس از آن وقتی بیمار به بیمارستان مراجعه می‌کند، اطلاعات روی سرور مرکزی بارگذاری می‌شوند و از روی کارت حذف می‌گردند تا فضا خالی شود [۲].

۵-۳ سازوکارهای امنیتی

از آنجایی که اطلاعات روی کارت هوشمند سلامت جزوی از اسرار هر فرد است و ممکن است کارت بیمار به طرق مختلفی از دسترس او خارج شود و در اختیار افراد خطرناک قرار بگیرد، لازم است تا با ایجاد سازوکارهایی از عدم دسترسی افراد غیر مجاز به اطلاعات روی کارت اطمینان حاصل کنیم. برای این منظور به بیان چالش‌ها و راهکارهای به کار رفته برای برطرف کردن آنها می‌پردازیم.

۵-۳-۱ چالش ها

عمده ترین چالش هایی را که در بحث کارت هوشمند سلامت با آنها روبرو هستیم، در ادامه شرح می‌دهیم [۷].

۵-۳-۱-۱ محرمانگی اطلاعات

اولین قدم برای برقراری امنیت، برآورد محرمانگی است. محرمانگی بدین معنی است که مهاجم نباید هیچ دانشی از محتوای اطلاعات موجود روی هر فضا از حافظه های روی کارت هوشمند که در قسمت های قبلی به تشریح آنها پرداختیم، به دست آورد.

۵-۳-۱-۲ تمامیت اطلاعات

در حالت کلی در مبحث امنیت ، موجودیتی "تمام" است که سه ویژگی زیر را داشته باشد:

- **یکپارچگی:** در تمامی مراحل خواندن از کارت و نوشتن روی آن، داده رد و بدل شده باید بدون تغییر باقی بماند. به عبارت دیگر، هرگونه تغییر احتمالی در اطلاعات روی کارت باید توسط خواننده اطلاعات قابل تشخیص باشد.
- **تازگی:** این ویژگی تضمین می‌کند که داده‌ی خوانده شده از روی کارت یا نوشته شده روی آن تکراری نمی‌باشد. این امر به جهت تضمین امنیت کارت در مقابل حملات تکرار مهم است.
- **صحت:** این ویژگی نیز تضمین کننده‌ی درستی اطلاعات در تمام طول فرایند خواندن و نوشتن می‌باشد.

۵-۳-۲ راهکارها

برای دادن پاسخ مناسب به دغدغه‌های اصلی در مورد امنیت کارت هوشمند، راهکارهای زیر ارائه می‌شوند.

۵-۳-۲-۱ امضاء دیجیتال

"امضای دیجیتال" به معنای یک شناسه الکترونیکی است که [۷]:

- با همان قدرت و تأثیر امضای دستی بکار رفته باشد.
- برای امضاکننده‌ی مجاز یکتا باشد.
- قابلیت تعیین اعتبار داشته باشد.
- فقط در کنترل امضاکننده مجاز باشد.

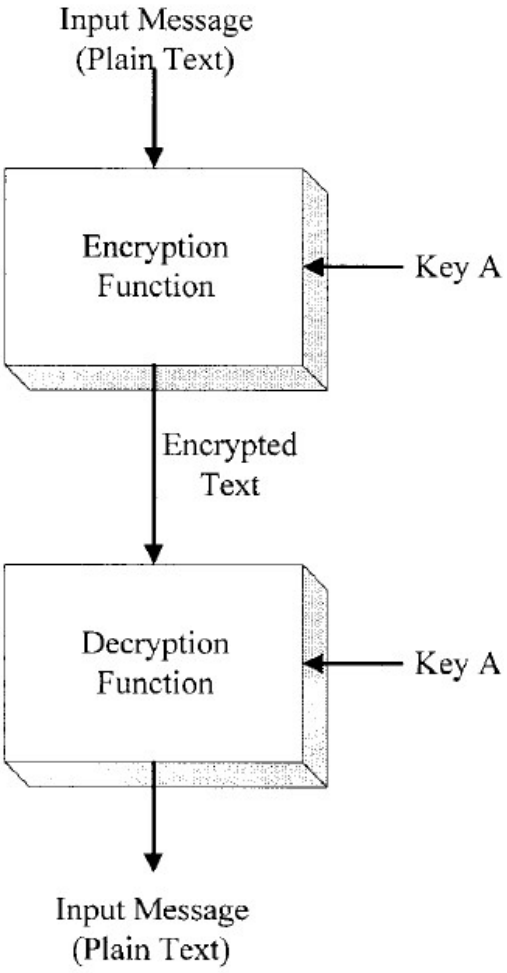
- به نحوی به نسخه الکترونیکی پیوند خورده باشد که اگر اطلاعات نسخه تغییر کند، امضاء بی اعتبار شود.
- با قوانین، مقررات و آیین نامه‌های امور دارویی مطابقت داشته باشد.

در دنیای الکترونیکی PKI[۴] می‌تواند با روشی قدرتمند که هم یکپارچگی و هم اعتبار صدور را تضمین کند، جایگزین رویکرد سنتی امضای دستی گردد. این روش یک اثر انگشت پرونده رایانه‌ای را با رمزگذاری کلید عمومی ترکیب می‌کند. رمزگذاری کلید عمومی سازوکاری برای رمزگذاری اطلاعات است که ابزاری مهم در ایجاد امضای الکترونیکی می باشد. الگوریتم رمزگذاری آن نامتقارن است یعنی آن که از دو کلید مجزا استفاده می‌کند. مالک یکی از دو کلید را خصوصی نگه می‌دارد و کلید دیگر را عمومی می‌کند. کلید عمومی تنها آنچه را کلید شخصی رمز کرده باشد می‌تواند رمزگشایی کند و چون هیچ کدام از کلیدها نمی توانند از کلید دیگر بدست آیند، عمومی بودن کلید دوم هیچ خطری ندارد.

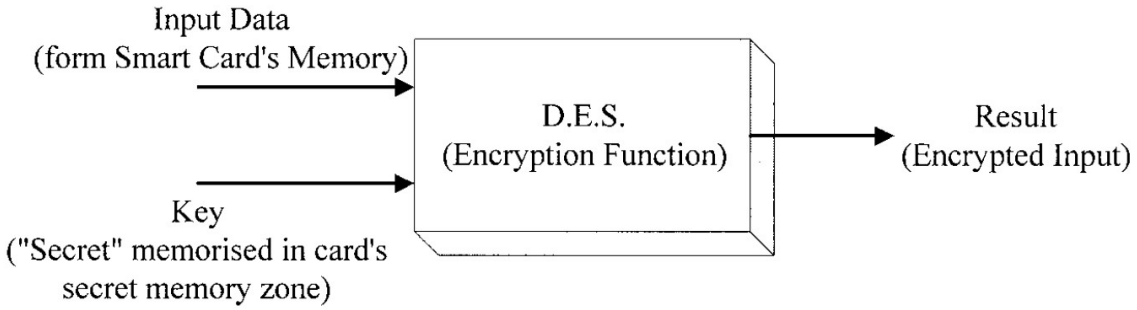
- **امضای سند:** در ابتدا رایانه فرستنده سند را از یک الگوریتم پیچیده عبور می‌دهد و یک خلاصه پیام با طول ثابت ایجاد می‌کند که آنرا اثر انگشت یکتای سند می‌نامند. حتی اگر یک حرف از سند تغییر کند، اثر انگشت هم متفاوت می‌گردد. سپس فرستنده کلید شخصی خود را برای رمز کردن این خلاصه بکار می‌برد. این خلاصه رمزشده که «امضای دیجیتال» نام دارد، اکنون به همراه پیام فرستاده می‌شود.
- **تأیید اعتبار امضاء:** گیرنده هنگام دریافت پیام رمز دیجیتالی شده از کلید عمومی فرستنده برای رمزگشایی امضاء و دستیابی به خلاصه پیام اصلی استفاده می‌کند. اگر امضا را بتوان با کلید عمومی فرستنده باز کرد می‌توان مطمئن بود که خود فرستنده آن را ارسال کرده است. این سازوکار قابلیت عدم انکار را فراهم می‌کند. سپس گیرنده یک خلاصه پیام جدید محاسبه می‌کند و با آن که تازه رمزگشایی شده است مقایسه می‌کند. اگر با هم تطابق داشته باشند نشانگر آن است که سند دستکاری نشده است و این یکپارچگی محتوایی را تضمین می‌کند. این فرایند به صورت آنی و شفاف در سیستم های PKI انجام می‌گیرد.

روشی دیگر برای رمزنگاری اطلاعات خام و رمزگشایی اطلاعات رمزشده، استفاده از یک الگوریتم رمزنگاری متقارن است که در شکل ۵-۲ نمونه‌ای از آن نشان داده شده است. یک الگوریتم رایج در رمزنگاری متقارن، الگوریتم DES است که با وجود پایین تر بودن امنیت آن، به علت سادگی پیاده‌سازی هنوز هم کاربردهای زیادی دارد. داده ها برای رمز شدن با کلیدی که فقط بیمار آنرا می‌داند، رمزنگاری می‌شوند و موقع رمزگشایی آنها در سمت دیگر، دقیقاً عکس همین فرآیند با دریافت کلید یکتای بیمار صورت می‌پذیرد و داده‌ی اولیه ایجاد می‌شود [۶]. نحوه ی رمز شدن اطلاعات توسط این الگوریتم به صورت جعبه سیاه در شکل ۵-۳ نشان داده شده است.

[4] Public key infrastructure



شکل ۵-۲: یک فرآیند رمزنگاری متقارن



شکل ۵-۳: پیاده‌سازی الگوریتم DES در یک کارت هوشمند

بخش ششم

جمع‌بندی، نتیجه‌گیری و پیشنهادات

۶-۱ جمع‌بندی و نتیجه‌گیری

در این مقاله سعی شد که به بررسی جنبه های مختلف مقوله‌ی سلامت الکترونیک و نحوه ی کارکرد کارت هوشمند سلامت الکترونیک پرداخته شود. در این راستا در ابتدا انواع کارت های هوشمند را بررسی کردیم، سپس پرونده های سلامت الکترونیک و سایر اجزا و استانداردهای این حوزه را معرفی نمودیم و در نهایت به بررسی معماری کارت هوشمندی که با یک سامانه‌ی سلامت الکترونیک تلفیق شده بود، معماری حافظه آن، و چگونگی مواجهه با محدودیت‌های این سامانه مثل کمبود فضای ذخیره‌سازی کارت و بررسی "امضای دیجیتال" که راهکاری برای مواجهه با چالش‌های امنیتی، به خصوص دو چالش اصلی "محرمانگی اطلاعات" و "تمامیت اطلاعات" است، پرداختیم.

۶-۲ پیشنهادات

یکی از مشکلات اساسی که در طول این پژوهش به آن پی بردیم، تعدد استانداردهای حوزه سلامت الکترونیک است که هرکدام توسط چندین مرکز خاص مورد استفاده قرار می‌گیرند و ضرورت ایجاد یک "استاندارد جهانی واحد" برای این حوزه و کدگذاری واحد اطلاعات پزشکی در پایگاه‌های داده کاملاً حس می‌شود و پیشنهاد می‌شود گروهی به طور خاص در آینده روی این زمینه کار کنند.

پیشنهاد دیگر استفاده از کارت‌های با ظرفیت بیشتر و در عین حال، هزینه‌ی کمتر برای توسعه معماری سیستم ارائه شده می‌باشد. در این راستا، به کارگیری سامانه NFC که می‌توانیم آنرا به نوعی یک کارت هوشمند نهفته در تلفن های همراه در نظر بگیریم، گزینه‌ی بسیار مناسبی می‌باشد.

منابع و مراجع

[1] G. Kardas and E. T. Tunali, “Design and implementation of a smart card based healthcare information system,” *Computer methods and programs in biomedicine*, vol. 81, no. 1, pp. 66–78, 2006.

[2] C. Lambrinoudakis and S. Gritzalis, “Managing medical and insurance information through a smart-card-based information system,” *Journal of Medical Systems*, vol. 24, no. 4, pp. 213–234, 2000.

[3] K. E. Mayes and K. Markantonakis, *Smart cards, tokens, security and applications*, vol. 2. Springer, 2008.

[4] K. Häyrinen, K. Saranto, and P. Nykänen, “Definition, structure, content, use and impacts of electronic health records: a review of the research literature,” *International journal of medical informatics*, vol. 77, no. 5, pp. 291–304, 2008.

[5] A. Roehrs, C. A. Da Costa, R. da Rosa Righi, and K. S. F. De Oliveira, “Personal health records: a systematic literature review,” *Journal of medical Internet research*, vol. 19, no. 1, p. e13, 2017.

[6] T. D. Gunter and N. P. Terry, “The emergence of national electronic health record architectures in the united states and australia: models, costs, and questions,” *Journal of medical Internet research*, vol. 7, no. 1, p. e3, 2005.

[7] R. Zhang and L. Liu, “Security models and requirements for healthcare application clouds,” in *2010 IEEE 3rd International Conference on cloud Computing*, pp. 268–275, IEEE, 2010.