

مجموعه مقالات دومین همایش

پژوهش در ثبت

جلد چهارم

فن آوری اطلاعات و ثبت احوال نوین

مرکز آموزش و پژوهش

سازمان ثبت احوال کشور

پاییز ۱۳۹۳

فهرست مطالب

صفحه	عنوان
۱	داده کاوی و استخراج دانش از داده های خام
۲۷	ده حمله برتر به پایگاه داده ها
۳۹	امنیت اطلاعات در آرشیو الکترونیکی اسناد هویتی ایرانیان
۵۰	نقش آفرینی ثبت احوال نوین در توسعه و پیاده سازی دولت الکترونیک
۷۰	بستر کاربردی شدن کارت هوشمند ملی

داده کاوی و استخراج دانش از داده های خام

امین محمودی^۱

چکیده

داده کاوی و کشف دانش یکی از رشته های کامپیوتری است که دارای رشد سریعی می باشد. محبوبیت آن به دلیل افزایش تقاضا جهت بدست آوردن ابزاری است که به تجزیه و تحلیل و درک مقدار عظیمی از داده ها کمک نماید. چنین داده هایی بطور روزانه توسط سازمان ثبت احوال، بانکها، شرکت های بیمه فروشگاهی خرده فروشی، بر روی اینترنت و اینترنت تولید می شود. این انفجار از میان استفاده روزافزون از کامپیوتر، اسکنر، دوربین های دیجیتال و... بوجود آمده است. ما در موقعیتی قرار داریم که منابع غنی از داده، انبار داده ها، پایگاه داده ها و سایر انبار داده ها براحتی در دسترس است. این به نوبه خود باعث می شود علاقه مندان زیادی از جوامع صنعتی و کسب و کار به این حوزه گرایش پیدا کنند. آنچه که بدان نیاز است متدولوژی روشن و ساده ای است که دانش را از داده های خام و پنهان استخراج نماید. این مقاله در برگیرنده یک مدل DMKD یکپارچه بر پایه فن آوری های در حال ظهور مانند OLE DB, DM, UDDI, SOAP, PMML, XML می باشد. این تکنولوژی ها باعث طراحی انعطاف پذیرتر و غیر خودکار و همچنین استفاده آسان از مدل DMKD می باشد و در واقع آن ها قادر به ساختن انبار دانش می باشند. آنها همچنین اجازه ارتباط بین چندین ابزار داده کاوی، پایگاه داده ها و انبار دانش را می دهند. آنها همچنین توانایی یکپارچه سازی و خود کار کردن وظایف DMKD را دارند [2].

^۱. اداره کل ثبت احوال استان فارس Amin_mahmoudy@yahoo.com

کشف دانش یک فرایند کوچک اما با اهمیت از شناسایی الگوهای قابل درک از مجموعه ای بزرگ از داده هاست که بصورت بالقوه مفید می باشد. یکی از مراحل استخراج دانش داده کاوی است ، داده کاوی مرحله ای است که در رابطه با استخراج واقعی دانش از داده می باشد. در مقابل آن ، فرایند عملیات استخراج دانش در رابطه با بسیاری از چیزهای دیگر از قبیل درک و آماده سازی داده ها ، تأیید و استفاده از دانش کشف شده است که اغلب برخی واژه های داده کاوی واستخراج دانش را به اشتباه مترادف می دانند. [2]

داده کاوی واستخراج دانش در سال ۱۹۸۹ در آزمایشگاه IJCAI با موضوع کشف دانش در پایگاه داده ها (KDD) به ارمغان آورده شد . پس از آن سال تا سال ۱۹۹۴ آزمایشگاه ها بکار خود ادامه دادند . در سال ۱۹۹۵ کنفرانس بین المللی کشف دانش و داده کاوی مهمترین رویداد سال برای DMKD شد . و چارچوب DMKD در دو کتاب " کشف دانش در پایگاه داده ها و پیشرفت در کشف دانش و داده کاوی " خلاصه شد، کنفرانس های داده کاوی واستخراج دانش مانند ACM -SIGKDD –SPIE –SIAM و مجلات مانند کشف دانش و داده کاوی ، دانش و سیستم های اطلاعاتی و نقش IEEE در مهندسی دانش و داده ها تبدیل به یک قسمت کامل از رشته DMKD شد [2].

با وجود پیشرفت های نظری در DMKD بدلیل تغییرات سریع در این رشته توصیف وضعیت فعلی آن آسان نمی باشد.

در این مقاله تلاش می کنیم وضعیت رشته DMKD را بر پایه سرویس اصل تحقیقات آنلاین مبتنی بر وب توصیف نمائیم.

سرویس اصل دسترسی به INSPCC و COPONDEX و PAYEONE و پایگاه داده اختراعات ثبت شده جهان را فراهم میکند و می تواند مقالات پژوهشی را با استفاده از مجموعه ای از کاربران مشخص گردیده از کلمات کلیدی و یک چارچوب زمانی پیدا کند.

انقلاب داده کاوی در اواسط دهه ۱۹۹۰ آغاز شد. مشخصاً در مدت زمان ۵ سال باعث افزایش مقالات از حدود ۲۰ تا ۱۲۷۰ می باشد که گواه این رشد سریع می باشد . یکی از دلایل این رشد ناشی از الحاق ابزارهای موجود و الگوریتم ها در یک چارچوب مشخص داده کاوی بود. اکثر ابزارهای داده کاوی بعنوان مثال یادگیری ماشین در حال حاضر بخوبی تثبیت شده است

تعداد مقالاتی که موضوعات یادگیری ماشین و داده کاوی را پوشش می دهد رشد آرامی دارد.

در سال ۲۰۰۰ تعداد ۷۴ مقاله که تعداد ۶ درصد تمام مقالات را شامل می شد. [2]

رشته DMKD حدود سال ۱۹۹۵ پدید آمد که در سال ۲۰۰۰ حدود ۱۵ درصد از تمام مقالات داده کاوی را تشکیل می داد. این لزوماً به این معنی نیست که فقط این درصد از پژوهش ها به داده کاوی و استخراج دانش اختصاص داده شده است از آنجائیکه خیلی از افراد هنوز هم داده کاوی و DMKD را یکی می دانند.

روند توسعه داده کاوی و استخراج دانش در چند سال گذشته شامل OLAP انبار داده ها ، قوانین انجمنی ، کارائی بالای سیستم های DMKD تکنیک های تجسمی و برنامه های کاربردی داده کاوی می باشد [2].

علاقه به پژوهش در قوانین انجمنی بدنبال یک الگوی عملی شبیه به حوزه داده کاوی است . از سوی دیگر پژوهش در OLAP (پردازش تحلیلی On Line) و انبار داده ها در ابتدا در حال رشد بود و در حدود سال ۱۹۹۹ بیشترین توجه به سمت آن بوده ، مشاهدات این است که برخی از روندها که در ابتدا بیشترین تأثیر را در زمینه داده کاوی داشته است شروع به کاهش کرده است . زیرا بیشترین مسائل مربوط به این حوزه ممکن است طی شده باشد و همچنین توجه به حوزه ها و برنامه های کاربردی جدید منتقل شده است . در سال های اخیر روند جدید ظهور کرده است که دارای پتانسیل بالقوه ای جهت بهبود حوزه DMKD می باشد مانند XML و فن آوری های مرتبط با XML مانند XML-PRC, PMML, UDDI محصولات پایگاه داده که ابزارهای داده کاوی را یکی می کند و پیشرفت های جدیدی در طراحی و پیاده سازی روند DMKD را در بردارد . اگرچه این ثابت شده است ، می بایست تلاش بیشتری برای توسعه بیشتر ابزارهای جدید داده کاوی انجام پذیرد که بتواند به مقدار بسیار عظیمی از داده های متنی ایجاد شده توسط اینترنت رسیدگی کند و یا بتواند دانش را از ابرمتن و تصاویر استخراج کند که اغلب در پزشکی با آن مواجه می شویم .

بطور خلاصه DMKD یک میدان در حال رشد بصورت تصاعدی با تأکید بر روی برنامه های کاربردی می باشد .

مدل های متفاوتی در خصوص داده کاوی و کشف دانش از قبیل CRISP-DM- Cabena و Cios مطرح می باشد که در این مقاله مدل ۶ مرحله ای CIOS که شامل مراحل درک حوزه

ودامنه مسئله ، درک داده ، آماده سازی داده ها، داده کاوی، ارزیابی دانش کشف شده و استفاده از دانش کشف شده می باشد و همچنین فن آوری ها و سرویس های نوظهور مانند DB-DM OLE, UDDI, SOAP, PMML, XML به همراه SOMiner و SOA, SOA+ مورد بحث و بررسی قرار می گیرد

از بین سیستم های هوشمند استخراج اطلاعات (OM) SOMINER مورد توجه است زیرا متمرکز به استخراج اطلاعات مفید از حجم زیادی داده است. ساخت سیستم های استخراج اطلاعات به صورت درجه بندی قابل گسترش ، قابل اجرا در داخل بخش و آسان ، کار دشواریست. یک طرح هماهنگ با سرویس برای استخراج داده ها که برای رسیدن به اهداف گسترش پذیری و قابلیت اجرای داخلی دستورالعمل های ساده ای به کاربران میدهند و پردازش کامپیوتری مقادیر زیادی داده را پشتیبانی مینماید SOMINER می باشد. یک طرح استخراج داده هماهنگ با سرویس که مهمترین فازهای فرایند کشف اطلاعات را هماهنگ میسازد. شامل پردازش داده ها ، استخراج داده ها (مدل سازی) ، فیلتر، معتبر سازی مدل و تجسم مدل می باشند. [3]

برخی از اهداف این موضوع و تحقیق عبارتند از:

- بسیاری از سازمان ها داده های زیادی جمع کرده اند با آن چه کنند؟ [1]
- بدیهی است با توجه به نرخ داده ها بکارگیری روش های سنتی که دستی و زمانبر هستند برای تحلیل آن ها کارساز نخواهند بود [1].

- شبکه سازی فرصتی مناسب و روبه رشد برای دسترسی بیشتر فراهم نموده است. [1]
- نیاز به تشخیص و پاسخ سریع با توجه به تکنولوژی های در حال ظهور قبل از رقبا وجود دارد [3].

همچنین ارائه روش و راهکارهایی است که بتواند:

- ارتباط بین ابزارهای متنوع داده کاوی و پایگاه داده را استاندارد می کند که ممکن است نسل جدید ابزارهای داده کاوی به تعدادی از محصولات مختلف پایگاه داده ارتباط برقرار نماید. [3]

- برای ساختن انبار داده استاندارد و اشتراک داده بین ابزار های مختلف داده کاوی که بروی پلتفورم های مختلف نرم افزاری کار می کنند، این درواقع کمک به تقویت موضوع و بحث DMKD و باز کردن دیدی برای کاربران جدید و برنامه های کاربردی جدید کمک نماید.

- برای پیاده سازی پروتکل های ارتباطی بین ابزارهای داده کاوی استفاده می شود که ممکن است منجر به توسعه مجموعه ابزارهای داده کاوی شود که این در واقع متشکل از ابزارهای مختلف داده کاوی که توسط شرکت های مختلف توسعه یافته است می باشد . اما قادر به برقراری ارتباط و ارائه پروتکلی برای استخراج تلفیقی ، قابل فهم تر ، دقیق تر و اجرا شدن آسانتر دانش می باشد.

- ارائه چارچوبی برای یکپارچه کردن و ارتباط بین مراحل مختلف DMKD می باشد. یک مسئله بسیار مهم این است که چگونه فرایند داده کاوی وکشف دانش را بدون پردازش دانش پیش زمینه گسترده وبدون دستکاری داده ها و دفترچه راهنما و تبادل داده ها بین برنامه های مختلف داده کاوی انجام شود. در واقع یکی دیگر از اهداف این موضوع و مقاله توصیف فن آوری است که ممکن است به خودکار سازی فرایند DMKD و همچنین آسانتر نمودن پیاده سازی آن کمک نماید

خودکار کردن یا واقع بینانه تر بگوئیم نیمه خودکار نمودن فرایند داده کاوی وکشف دانش کار بسیار پیچیده ای می باشد. ورودی هایی که توسط کاربر جهت فرایند DMKD داده می شود. امری ضروری جهت فرایند DMKD می باشد . از آنجا که فقط کارشناسان این حوزه دانش لازم درباره وسعت کار و داده ها را دارند ورودی ها آنها با اهمیت می باشد . همچنین ارزیابی نتایج در هر مرحله نیاز است.چندین فن آوری برای خودکار کردن فرایند DMKD ضروری می باشد.که به شرح ذیل می باشد

- یک انبار داده که ذخیره داده دانش پیش زمینه و مدل ها را در بر دارد.

- قراردادی جهت مبادله داده و اطلاعات بین انبار داده و ابزار داده کاوی و ابزار مختلف داده را فراهم نماید.

- استاندارد هایی برای توصیف مدل داده

از دیگر اهداف این موضوع در واقع ارائه معماری های مبتنی بر وب می باشدکه ابزار داده کاوی می توانند از آن استفاده نمایند ،معماری های مذکور بر پایه XML می باشند کاربرد این

فن آوری ها تا حدود زیادی به خودکار سازی فرایند استخراج دانش و ایجاد ارتباط بین ابزارهای داده کاوی و همچنین ایجاد جستجوهای پویا می باشد. از همه مهمتر اینکه بتوان ابزارهایی برای فرایند استخراج دانش جدا از این مسئله که سخت افزار و پلتفورم چه باشد ارائه نمود. ابزارهای مبتنی بر پروتکل XML دارای این ویژگی می باشند.

کاربردهای موضوع تحقیق در موارد ذیل می باشد:

اطلاعات کسب و کار، تحلیل داده های بازاریابی و فروش، تحلیل سرمایه گذاری، تأیید وام، تشخیص تقلب، اطلاعات ساخت و تولید، کنترل و زمانبندی، مدیریت شبکه، پایگاه داده های پزشکی و...

طراحی و پیاده سازی نسل جدیدی از سیستم های با کارایی بالا ی داده کاوی که ترکیب چندین روش داده کاوی هستند ، و قادر به استخراج منابع دانش ناهمگن مانند داده های چند رسانه ای ، می تواند نتایج را نشان داده و مقادیر عظیمی از داده های پیچیده را بررسی کنند. یکی از اهداف طراحی سیستم ها باید این باشد که طراحی رابط کاربر بهتر شود. نتیجه این کار پذیرش بیشتر محصولات را به دنبال دارد، به خصوص توسط شرکت های متوسط و کوچک که در آن کاربران ممکن است مهارت های فنی محدودی را داشته باشند. یکی دیگر از موضوعات بسیار مهم درک کاربر از تازگی، فهم و سادگی دانش تولید شده بوسیله پردازش های DMKD است.

مواجه شدن با حجم بسیار وسیعی از داده ها و ایجاد انبارهای داده در سالهای اخیر و مشکلات بازیابی دانش مخفی موجود در آنها جهت بکارگیری این اطلاعات در راستای اهداف مدیریتی سبب شد که تکنیک های داده کاوی و استخراج دانش و اهمیت این موضوع در مجامع علمی مورد توجه قرار گرفته شود [1].

داده ها سریعاً در حال تغییر و بی ثبات هستند و ممکن است ابزارهای قبلی داده کاوی در جهت استخراج دانش بی اعتبار شوند، بعلاوه متغیرهای اندازه گیری شده در یک پایگاه داده ممکن است با اندازه گیری های جدید در طول زمان اصلاح شده حذف و یا افزایش یابند. همچنین اگر پایگاه داده از ابتدا با هدف کشف دانش طراحی نشده باشد ممکن است فاقد برخی ویژگی های مهم باشد [1].

داده کاوی و استخراج دانش از داده‌های خام ۷

بسیاری از روش‌ها و ابزارهای فعلی کشف دانش واقعا تعاملی نیستند و نمی‌توانند به آسانی دانش پیشین درباره یک مسئله را در نظر بگیرند. استفاده از دانش حوزه مورد مطالعه در همه مراحل فرایند DMKD مهم است. بسیاری از ابزارهای داده کاوی به تنهایی مفید نبوده و بهتر است با سایر سیستم‌ها تلفیق و یکپارچه شود.

مشکل دیگر فن آوری‌های قدیمی این بود که به اشتراک گذاری مدل داده به آسانی امکان پذیر نیست همچنین بسیاری از روش‌ها وابسته به پلتفرم می‌باشد که این بکارگیری موثر ابزارهای داده کاوی و استخراج دانش را با چالش مواجه می‌کند. از دیگر مشکلات میتوان مثلا به اینکه آیا داده صحیح با فرمت صحیح دریافت شده یا نه و اینکه آیا داده دقت لازم را دارد یا نه. داده ممکن است کامل نباشد و بسیاری از مقادیر را نداشته باشد اشاره کرد. مشکل دیگر کامل نبودن ابزارها است و همچنین توسعه تکنیکهای انطباقی است. البته تحقیقات بسیاری در این زمینه شده است اما راه درازی تا دستیابی به ابزارهای قدرتمند تجاری داریم [1].

می‌توان به اختصار برخی مشکلات این حوزه را به شرح ذیل عنوان نمود:

-عدم وجود جستجوی پویا

-عدم ارتباط بین ابزارهای داده کاوی و جعبه ابزار داده کاوی

-وجود محاسبات پیچیده

-خودکار نبودن عملیات DMKD

-عدم وجود جعبه ابزارهای کاربردی و انعطاف پذیر

-عدم وجود روشهای یکپارچه جهت انجام فرایند DMKD

از طرفی، با گسترش روز افزون اینترنت، میزان استفاده از مستندات XML بویژه در مبادله داده بسیار زیاد شده و تعداد مستندات XML موجود در اینترنت روز به روز در حال افزایش می‌باشد. لذا با توجه به حجم و تعداد بسیار زیاد اینگونه مستندات وجود روش‌هایی جهت داده کاوی از مستندات XML بسیار ضروری و مورد نیاز است. داده کاوی از مستندات XML بسیار پیچیده تر و مشکل تر از داده کاوی جداول رابطه ای می‌باشد. از جمله مشکلات داده کاوی در XML میتوان به طبیعت پویا، وجود ساختارهای ناهمگون و حجم زیاد مستندات XML اشاره کرد. از طرفی بواسطه استاندارد و فراگیر بودن XML، راهکار ارائه شده برای داده کاوی مستندات XML میتواند بسیار با ارزش بوده و در طیف وسیعی از کاربردها استفاده شود.

اما جدا از فن آوری ها معمولاً خود مدل ها نیز داری مشکلاتی جهت اجرای فرایند DMKD بوده اند مثلاً مدل پیچیده تر شبیه مدل نه مرحله ای پیشنهاد شده FAYYAD و همکاران می باشد زیرا بیش از حد مراحل ارزیابی و استفاده از دانش کشف شده در این مدل تکرار شده است و یا مدل Cabena که مرحله درک داده در آن از قلم افتاده است و یا سایر مدل ها که کاربردی نمی باشند این موارد مشکلاتی در مدل های داده کاوی و استخراج دانش بوده که نیاز به یک مدل کاربردی و ساده و درعین حال کامل را ایجاد می نمود. که در این مقاله بطور کامل شرح داده می شود [4]

برای حل مشکلات مدل های فوق الذکر مدل شش مرحله ای CIOS شرح داده می شود.

شش مرحله فرایند DMKD در زیر توضیح داده شده است : [5]

۱- درک حوزه یا دامنه مسئله

در این مرحله از نزدیک با کارشناسان حوزه مسئله تعریف و اهداف پروژه تعیین می گردد. افراد کلیدی شناسایی و یادگیری درباره راه حل های موجود انجام می شود این در برگیرنده اصطلاح یادگیری دامنه خاص می باشد. شرح مشکل از جمله محدودیت های در روند پروژه می باشد. سپس اهداف پروژه بایستی به اهداف DMKD تبدیل شود و ممکن است شامل انتخاب اولیه از ابزارهای بالقوه داده کاوی باشد .

۲- درک داده :

این مرحله شامل مجموعه ای از داده های نمونه می باشد و تصمیم گیری در مورد اینکه کدام داده نیاز خواهد شد از جمله اندازه و فرمت آن ، اگر دانش پس زمینه ای وجود دارد برخی از ویژگی ها ممکن است مهمتر از بقیه در نظر گرفته شود . پس ما نیاز به سودمندی داده ها در رابطه با اهداف DMKD داریم . نیاز است که داده ها بررسی شوند از لحاظ کامل نبودن ، افزونگی ، فاقد ارزش ، معقول بودن و مقدار خصوصیات و غیره ...

۳- آماده سازی داده ها

این گام مهمی است که بر اساس آن موفقیت کل فرایند کشف دانش به آن بستگی دارد . معمولاً حدود نصف تلاشها انجام پروژه صرف این مرحله می شود در این مرحله تصمیم گیری می شود که چه داده ای برای مرحله ۴ ابزارهای داده کاوی به عنوان ورودی در نظر گرفته شود. این ممکن است نمونه برداری از داده ها ، اجرای آزمون های همبستگی و اهمیت ، پاکسازی

داده‌ها مانند چک کردن کامل بودن یک رکورد، حذف اغتشاش و غیره باشد. داده‌های تمیز را می‌توان بیشتر با انتصاب ویژگی و استخراج دانش (به منظور کاهش اندازه) بوسیله استنتاج از ویژگی‌های جدید (مجزا کردن) و بوسیله خلاصه‌سازی داده‌ها (ریز ریز کردن داده) بدست آورد که نتیجه رکورد جدیدی از داده‌ها خواهد بود. داشتن وردی خاص از الزامات مورد نیاز برای برنامه ریزی و استفاده از ابزارهای داده کاوی می‌باشد.

۴- داده کاوی

یکی دیگر از گام‌های کلیدی در فرایند کشف دانش می‌باشد، اگرچه این ابزار داده کاوی است که اطلاعات جدید را استخراج می‌کند، اجرای برنامه‌های آن معمولاً زمان کمتری نیست به آماده‌سازی داده‌ها در بر می‌گیرد. این مرحله شامل استفاده از ابزارهای برنامه‌ریزی داده کاوی و انتخاب یکی از آن‌هاست. داده کاوی شامل بسیاری از انواع الگوریتم‌ها مانند مجموعه‌های فازی، روش‌های بی‌زی، محاسبات تکاملی، یادگیری ماشین، شبکه‌های عصبی، خوشه‌بندی، تکنیک‌های پردازش و غیره می‌باشد. این مرحله شامل استفاده از ابزارهای مختلف داد ه کاوی بر روی داده‌ها تهیه شده در مرحله ۳ می‌باشد. مدل‌های داده‌های تولید شده با استفاده از روال‌های آزمایشی تأیید می‌گردد.

یکی از مشکل‌های عمده این مرحله این است که ممکن است بسیاری از ابزارهای خارجی در دسترس کاربر نباشد یا اینکه ابزارهای معمول برای استفاده از حجم عظیمی از داده‌ها توانایی نداشته باشد که دومی یک مسئله بسیار مهم است. میزان مقایسه ابزارهای داده کاوی بوسیله افزایش خطی زمان اجرا مشخص می‌شوند با افزایش نقاط دیتا در یک مقدار ثابت، حافظه در دسترس مشخص می‌گردد.

رویکرد‌های اخیر برای اندازه‌گیری طرز رفتار ابزارهای داده کاوی وابسته به چارچوب Meta-Mining می‌باشد Meta-Mining باعث بوجود آمدن Meta-Knowledge از دانش تولید شده توسط ابزار داده کاوی می‌باشد.

بوسیله تقسیم داده‌ها به زیر مجموعه‌ها، مدل‌های داده بوسیله زیر مجموعه‌ها تولید می‌شود و توسط این مدل‌های داده، فرا دانش تولید می‌شود. در این رویکرد مدل‌های داده کوچک بعنوان داده‌های ورودی بجای مقدار بسیار عظیمی از داده‌های اصلی می‌باشد که این تا حد زیادی باعث کاهش بار محاسباتی می‌شود.

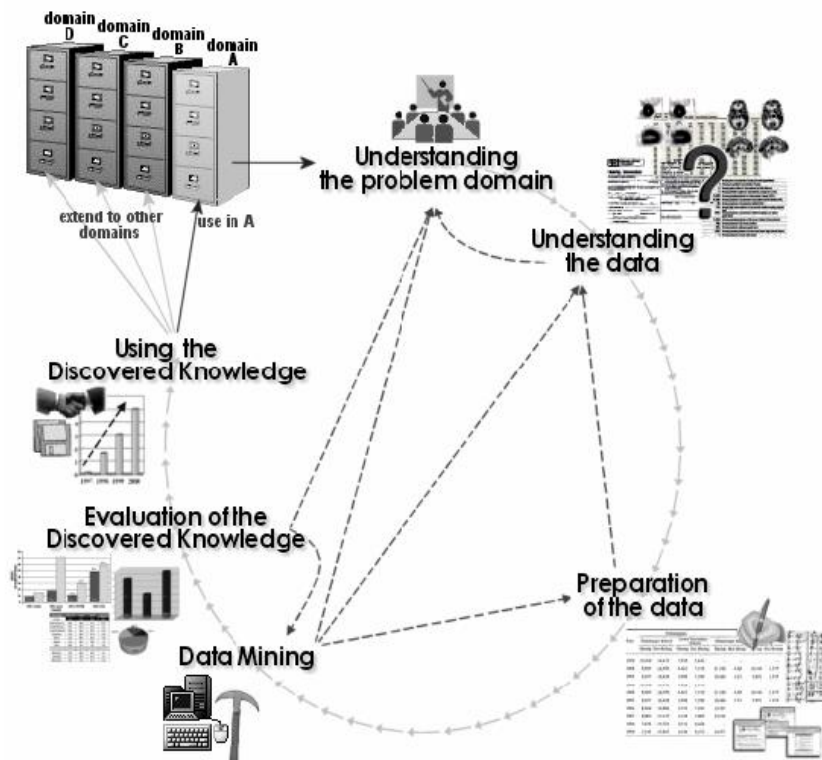
۵- ارزیابی دانش کشف شده

این مرحله شامل درک نتایج، چک کردن اینکه آیا اطلاعات جدید و بدیع و مطابق با خواسته ها می باشد انجام می گردد. در این مرحله تفسیر نتایج بوسیله افراد خبره این حوزه و بررسی تأثیر دانش کشف شده می باشد. تنها مدل های تأیید شده (استفاده از نتایج بسیاری از ابزارهای داده کاوی) در این مرحله حفظ می شوند. ممکن است فرایند کامل DMKD برای شناسایی عملیات جایگزین بازبینی شود. تا نتایج بهبود پیدا کند. لیستی از مغایرت ها توسط این مرحله فرایند ساخته می شود.

۶- استفاده از دانش کشف شده

این مرحله بطور کامل در دست مدیر پایگاه داده است. این مرحله متشکل از برنامه ریزی برای چگونگی استفاده از دانش کشف شده می باشد. حوزه کاربردی در محدوده جاری می بایست به حوزه های دیگر توسعه یابد. برنامه ای برای نظارت بر اجرای دانش کشف شده باید ایجاد شود و کل پروژه باید مستند شده باشد.

مدل فرایند DMKD در شکل ۱ توضیح داده شده است مسئله مهم تکراری و تعاملی بودن این روند است. از آنجا که هر تغییرات و تصمیمات اتخاذ گردیده در هر مرحله می تواند باعث تغییر در مرحله های بعدی شود. حلقه های بازخورد ضروری می باشد. چند مدل شناسایی شده برای مکانیسم بازخورد به شرح ذیل می باشد.



شکل ۱

- از مرحله ۲ به مرحله یک بدلیل حوزه دانش اضافی ممکن است درک بهتر داده ها مورد نیاز باشد.
- از مرحله ۳ به ۲ بدلیل آنکه اطلاعات اضافی یا مشخص تر در مورد داده ها وجود دارد ممکن است قبل از انتخاب الگوریتم پردازش داده های خاص مورد نیاز باشد(برای نمونه تبدیل داده ها یا مجزا کردن)
- از مرحله ۴ به ۱ زمانی که انتخاب ابزار داد ه کاوی تولید نتایج رضایت بخش نیست پس در نتیجه اهداف پروژه می بایست اصلاح شود.
- از مرحله ۴ به ۲ در یک وضعیت هنگامی که دیتا اشتباه باعث شکست ابزار داد ه کاوی شود (بعنوان مثال داده مرحله ۳ بعنوان گسسته یا پیوسته تشخیص داده نمی شود.) رایجترین سناریو وقتی است که واضح نسیت کدام ابزار داد ه کاوی باید استفاده شود زیرا درک ضعیفی از داده ها در دسترس است.

- از مرحله ۴ به ۳ آماده سازی دیتا بدلیل شرایط خاص استفاده از ابزار داده کاوی که ممکن است در طول مرحله آماده سازی داده ها شناخته نشود، بهبود پیدا می کند.

- از مرحله ۵ به یک زمانی که دانش کشف شده معتبر نیست ، چندین دلیل برای این وضعیت امکان دارد : درک نادرست یا تغییر نادرست دامنه ،طراحی نادرست یا درک محدودیت های مسئله ، الزامات یا اهداف ، در این موارد نیاز است که تمام روند DMKD تکرار شود.

- از مرحله ۵ به ۴ زمانی که دانش کشف شده جدید مفید و جالب نیست در این مورد ممکن است ابزار داده کاوی متفاوتی انتخاب گرددو مرحله ۴ برای استخراج دانش نو ، مفید و جدید تکرار گردد.

مسیرهای بازخورد به عنوان خطوی تیره در شکل ۱ نشان داده شده است. مسیرهای بازخورد شرح داده شده به هیچ وجه جامع نمی باشد.

مراحل مشترک برای سه مدل عبارتند از درک دامنه ، داده کاوی ، ارزیابی دانش کشف شده مدل Fayyad بسیار دقیق و ممکن است بیشترین راهنمایی را ارائه کند. مرحله ۵ و ۶ بیش از حد در این فرایند آمده است و تکرار شده است، ما فکر می کنیم که این مرحله را بایستی در طی مراحل درک حوزه و درک داده برای هدایت روند آماده سازی داده انجام داد.

[4]

به عبارت دیگر هدف از آماده سازی داده ها ، آماده کردن داده ها جهت استفاده با ابزار داده کاوی انتخاب شده می باشد. در حالیکه مدل های پیشنهادی آن با ابزار داده کاوی انتخاب شده را در مرحله ۶ با توجه به نتایج حاصل از آماده سازی داده ها در نظرمی گیرد. و این ممکن است باعث ایجاد مشکل در زمانی که داده آماده شده برای ابزار داده کاوی انتخاب شد مناسب نباشد شود. بنابراین یک حلقه بازخورد غیرضروری ممکن است برای تغییر آماده سازی داده ها در مرحله ۳ و ۴ لازم باشد.

یک مسئله بسیار مهم این است که چگونه فرایند DMKD را بدون پردازش دانش پیش زمینه گسترده بدون دستکاری داده ها و دفترچه راهنما و تبادل داده ها بین برنامه های مختلف داده کاوی انجام شود. دو بخش بعدی توصیف فن آوری است که ممکن است به خودکار سازی فرایند DMKD و همچنین پیاده سازی آسانتر کمک می کند. [5]

XML

مورد مطالعه گسترده در چندین سال اخیر قرار گرفته است. این تکنولوژی به همراه تکنولوژی‌های دیگر که در بالای XML قرار گرفته اند مانند UDDI, SOAP, XML-PRC, PMML می‌توانند راه حل‌هایی را جهت نیمه خودکار سازی فرایند DMKD فراهم نمایند. در ادامه این تکنولوژی‌ها معرفی و برنامه‌های آن‌ها در روند DMKD شرح داده می‌شود. اگر چه تکنولوژی‌هایی مانند OLEDB-DM, OLAP و تأثیر آنها نیز بفرایند DMKD مورد بحث قرار می‌گیرد.

XML

یک زبان نشانه گذاری برای اسناد حاوی اطلاعات ساخت یافته می‌باشد. اطلاعات ساخت یافته متشکل از محتویات (اعداد ، رشته‌های کاراکتری ، عکسها و ...) می‌باشد و اینکه اطلاعات چه نقش‌هایی می‌تواند باز می‌کند. محتویات اطلاعات (بعنوان مثال یک قاعده از انتخاب گره‌های ساخته شده است و یک انتخابگر یک جفت از صفات (نام و ارزش) می‌باشد. XML یک استاندارد برای اضافه کردن نشانه گذاری تعریف میکند یا به عبارتی دیگر برای شناسایی ساختار در اسناد و مدارک بکار می‌رود. XML در درجه اول برای ایجاد وبه اشتراک گذاری و پردازش اطلاعات مورد استفاده قرار می‌گیرد. XML کاربران را برای تعریف برچسب نشانه که ویژه یک هدف خاص می‌باشد قادر می‌سازد. تگ‌های XML برای توصیف معنا و یا چارچوب داده‌ها در شیوه‌ای دقیقاً تعریف شده مورد استفاده قرار می‌گیرد. این ویژگی‌های مدل سازی است که XML را محبوب می‌کند. به لطف این ویژگی پردازش اسناد XML می‌تواند بصورت خودکار انجام شود. تکنولوژی XML بطور گسترده‌ای در صنعت و انتقال و اشتراک اطلاعات مورد استفاده قرار می‌گیرد. یکی از مهمترین خصوصیات XML این است که DBMS‌ها با XML استاندارد پشتیبانی می‌شوند. از نقطه نظر DMKD این بدان معنی است که XML به عنوان یک رسانه نقل و انتقال می‌تواند بین ابزارهای داده کاوی و XML مبتنی بر انبار داده‌ها استفاده شود که برای ذخیره دانش کشف شده و اطلاعات مربوط به داده‌ها و DBMS‌هایی که داده را ذخیره می‌کنند استفاده شود. یکی از دیگر مزایای XML توانایی پرس و جو برای بازیابی و دستکاری داده ذخیره شده در سند است. تعدادی از زبان‌های پرس و جو توسعه یافته

عبارتند از : Corel,quilt,unql,xduce,xml-QI,XPATH,xql,Xquery,Yatl که دو زبان پرس وجو Xpath,Xqurey موفق به تأیید C۳W می باشند. [2]

XML-PRC

یک پروتکل است که اجازه می دهد نرم افزار در حال اجرا بر روی سیستم های ناهمگون و در محیطهای مختلف بروش فراخوانی از طریق اینترنت انجام شود. این فن آوری از http برای انتقال و XML برای رمز گذاری استفاده می کند. XML-PRC طراحی شده است که بسادگی امکان اجازه انتقال ، پردازش و ساختمان داده های پیچیده را بدهد. پیاده سازی XML-PRC تقریباً در دسترس تمام سیستم عامل ها ، زبان های برنامه نویسی محیطهای ایستا و پویا که شامل پیاده سازی در پرل ،پیتون ، جاوا Microsoft و Delphi می باشد [2] .

SOAP

یکی دیگر از پروتکل های مبتنی بر XML/http برای دسترسی به خدمات ، اشیاء و سرور در اینترنت است و مستقل از پلتفورم است و شامل ۳ بخش می باشد. یک پاکت که تعریف چارچوب و توصیف چیزی است که در یک پیام است و چگونگی پردازش آن با دو مجموعه از قواعد رمزگذاری برای بیان نمونه هایی از انواع داده تعریف شده در برنامه و پیمان نامه ای که نشان دهنده روال های فراخوان راه دور و پاسخ آن می باشد. SOAP از XML-PRC بدست آمده است و آن یک مجموعه بزرگ از XML-PRC می باشد اما آنها با هم سازگار نیستند. [2]

از نقطه نظر DMKD هر دو پروتکل XMI-PRC و SOAP می توانند بعنوان پروتکلی برای ارتباط بین ابزارهای داده کاوی به منظور ایجاد جعبه ابزار داده کاوی مورد استفاده قرار گیرند. چنین جعبه ابزارهایی از ابزارهای داده کاوی متنوع استفاده می کند. انتخاب هر یک که مناسب برای کار با داده عرضه شده و نتایج ترکیب شده را بدون ضرورت اینکه دیتا بطور جداگانه توسط ابزار های داده کاوی انتخاب شوند تأمین می کند با استفاده از این پروتکل جعبه ابزار داده کاوی می تواند بر روی اینترنت در دسترس ابزارهای داده کاوی قرار گیرد. بعنوان یک نتیجه توزیع شده و سفارشی شده توسط کاربر جعبه ابزار براحتی ساخته می شود .

PMML

یک زبان مبتنی بر XML است که در تعریف مدل های پیش بینی و به اشتراک گذاری در میان برنامه های کاربردی سازگار استفاده می شود. توسط گروه داده کاوی مستقل از رهبری

گروه می باشد که استانداردهای داده کاوی را توسعه می دهد. اعضای آن از-SPSS-ORACLE-IBM و سایرین می باشد.

PMML

روش فروشنده مستقل برای تعریف مدل ها را تعریف می کند. آن مسائل مربوط به ناسازگاری بین برنامه های کاربردی و فرمت های اختصاصی را حذف می کند. این به نوبه خود تبادل مدل ها بین برنامه های کاربردی را میسر می کند بعنوان مثال به کار بران اجازه می دهد تا مدل های داده را بوسیله فروشنده نرم افزار تولید کنند و پس از آن دیگر فروشنده نرم افزار از تجزیه و تحلیل استفاده کند در عین حال دیگری مدل ها را از ریابی و دیگر فروشنده مدل را تجسم کند. در عین حال یکی از عناصر خیلی مهم توانایی ساختن جعبه ابزار داده کاوی می باشد.

راه حل های قبلی برای مشکل به اشتراک گذاری مدل داده ها در سیستم های سفارشی ساخته شده گنجانیده شده بود و در نتیجه تبادل مدل ها با یک برنامه در خارج از این سیستم عملاً غیر ممکن بود.

PMML

در حال حاضر از مدل های داده کاوی ذیل پشتیبانی می کند:

درخت تصمیم گیری، مدل های بیز، رگرسیون ، دنباله و قوانین انجمنی شبکه های عصبی ، توزیع های مبتنی بر الگوریتم های خوشه بندی PMML مدل ها را بوسیله ۸ ماژول توصیف می کند. هدر ، شمای داده ، شمای داده کاوی، شمای مدل پیش بینی تعریف برای مدل های پیش بینی ، تعریف برای گروه مدل ها قوانین برای انتخاب و ترکیب مدل ها و گروهها و قوانین پردازش استثناء

PMML

نه تنها چندین مدل داده کاوی را پشتیبانی می کند بلکه همچنین از گروه مدل ها و مکانیسم انتخاب و ترکیب مدل ها نیز پشتیبانی می کند [2].

UDDI

استخراج توضیحات و یکپارچگی همگانی (UDDI) یک چارچوب مستقل از Platform برای توصیف استخراج و یکپارچگی خدمات با استفاده از اینترنت و عملیات رجیستری می باشد. این

چارچوب از http-soap-xml و پرتکل های DNS استفاده می کند. در حال حاضر بالغ بر ۲۲۰ شرکت از UDDI استفاده می کنند از UDDI می توان در مواردی مثل پیدا کردن سرویس درست از میان میلیون ها سرویس در دسترس کمک گرفت و یا ارتباط با یک سایت وب سرویس با استفاده از WSDL را فراهم نماید که از فرمت های مبتنی بر XML برای توصیف سرویس های شبکه استفاده می کند در هر زمان بدلیل مزایایی مانند رسیدن به مشتریان جدید ، گسترش ارائه خدمات و رسیدن به بازار با تقریباً قطعی است که ارائه دهندگان خدمات ، خدمات خود را با استفاده از UDDI ثبت نمایند. جعبه ابزار داده کاوی سپس از جهت در دسترس بودن ابزار های آنلاین داده کاوی با استفاده از UDDI بررسی می شود و باعث فراخوانی آنها می شود که می تواند نتایج معنا داری برای ارائه جهت پردازش داده شود. ابزارهای داده کاوی (سرویس) داده های ارائه شده را بوسیله جعبه ابزار داده کاوی برمی دارد و پردازش می کند و نتیجه را به جعبه ابزار بر می گرداند با استفاده از این پروتکل جعبه ابزار داده کاوی بصورت پویا می تواند در دسترس و چندین ابزار داده کاوی را استفاده کند که پردازش داده و تولید نتایج را در بر دارد. جعبه ابزار نتایج را جمع آوری آنها را پردازش و به کاربر ارائه و نهایتاً آنها را پایگاه دانش ذخیره می کند. این مکانیزم ساده که توسط پیدا کردن پویا ابزار آنلاین داده کاوی می باشد می تواند در ساخت جعبه ابزارهای کاربردی و انعطاف پذیر مورد استفاده قرار گیرد.

فن آوری فوق قطعاً در نتیجه خودکار کردن DMKD کمک می کنند . XML را می توان جهت ذخیره دیتا استفاده کرد PMML برای ذخیره مدل داده بکار می رود SOAP و XML- PRC برای ارتباط بین برنامه های کاربردی متفاوت داده کاوی مستقل از پلتفرم استفاده کرد و UDDI را می توان برای پیدا کردن خدمات داده کاوی ارائه شده توسط شرکت های داده کاوی استفاده کرد. توضیحات بیشتر در مورد چگونگی ترکیب فن آوری های در روند DMKD در زیر داده شده است. یک مزیت بزرگ تکنولوژی های بالا این است که Open source می باشند و می توانند بصورت آزاد آنها را دانلود کرد و استفاده نمود .

OLAP

(پردازش تحلیلی بر روی خط) یک تکنولوژی نسبتاً قدیمی DMKD است. هدف اصلی OLAP این است که به کاربران دیدگاه چند بعدی از مجموعه داده ها برای دسترسی سریع به اطلاعات مورد نیاز برای تجزیه و تحلیل بیشتر را می دهد.

OLAP

سرعت ، سازگاری ، دسترسی و تعامل به انواع دیدگاه ها برای هرگونه اطلاعات را به ما می دهد. OLAP و انبار داده (data warehouse) فن آوری های مکمل هستند . یک data warehouse داده ها را ذخیره و مدیریت می کند در حالیکه OLAP دیتا را به حداکثر به اطلاعات استراتژیک تبدیل می کند. محدوده سرویس های OLAP از راهبری ابتدایی و در حال مرور داده تا تجزیه تحلیل از قبیل پردازش سری زمانی می باشد. OLAP به کاربر قدرت تصمیم گیری می دهد.

از رایجترین کاربردهای OLAP بازاریابی، تبلیغات ، تجزیه و تحلیل مشتری ، پیش بینی فروش و تقسیم بندی مشتریان است. OLAP دارای ویژگی های زیر است

- دیده‌های چند بعدی که کمک به پردازش تحلیلی داده از میان اطلاعات انعطاف پذیر در دسترس می دهد.

- هوش زمانی به این معنی که سیستم های OLAP می توانند با ماهیت محتوای آنان مقابله کنند مفهوم زمان را باید به عنوان یک ویژگی جدا ناپذیر هر بسته تحلیل در نظر گرفته شود.

- محاسبات پیچیده : که به کاربر یک ابزار برای مثال تسهیم محاسبات (درصد از کل) ، اعتبارات ، که آنها با استفاد از الگوریتم های روند مانند میانگین حرکت و درصد رشد انجام می شود.

همچنین فن آوری OLAP را می توان بطور مستقیم با اکثر الگوریتم های داده کاوی مانند قوانین انجمن، طبقه بندی پیش بینی و خوشه بندی یکپارچه نمود. OLAP بخوبی با داده کاوی جفت و همراه می شود زیرا انبار داده متفاوت از DBMS رابطه ای سنتی طراحی شده است. انبار داده یک انبار مرکزی اطلاعات است که مدل داده یکپارچه برای دیتا که معمولاً در چند مکان مختلف ذخیره می شود می باشد. این تکنولوژی موضوع گرا فقط خواندنی از داده

های قدیمی می باشد. این نه تنها تضمین ثبات داده هاست همچنین به پرس وجو موثر در جهت ذخیره داده انعطاف می دهد [2].

OLE DB-DM

فرمتی از پرس و جو های زبان SQL است که به کاربران اجازه آموزش و تست مدل های داده کاوی را می دهد. کاربرد اصلی آن برای استفاده از ابزار های مختلف داده کاوی بوسیله یک API مشترک است. OLE DB-DM از رایجترین ابزار داده کاوی پشتیبانی کرده و شامل تجزیه و تحلیل داده کاوی دقیقاً برخلاف پایگاه داده رابطه ای است. OLE DB-DM از این عناصر تشکیل شده است:

Data mining model (DMM)

که توسط یک جدول رابطه ای مدل سازی شده با این تفاوت که شامل دو ستون اضافی است که از این ستونها برای آموزش و پیش بینی استفاده می شود. پس از درج اطلاعات در جدول، یک الگوریتم داده کاوی آنها را پردازش و مدل داده کاوی ذخیره می شود. به این ترتیب، DMM قابل نمایش، تعریف مجدد و یا قابل استفاده توسط یک کاربر می باشد.

Prediction join operation

پیش بینی متصل به عملیات: عملیاتی متصل به query بین مدل داده کاوی و داده بوده که برای تولید یک نتیجه قابل پیش بینی می تواند بعنوان یک رکورد OLE DB و یا یک رکورد ADO به کاربر فرستاده شود.

OLE DB-DM schema rowsets

، که به برنامه های کاربردی کاربران اجازه جستجوی مدلها و سرویسهای داده کاوی موجود را میدهد .

یکی از مزایای استفاده از OLE DB-DM، پشتیبانی از انواع داده جهت داده کاوی توسط نوعی flags به جای استفاده از داده های SQL می باشد. از انواع داده های زیر پشتیبانی می شود:

key

(کلید) - صفت گسسته که یک کلید است.

continuous

(پیوسته) - - ویژگی با ارزش های پیوسته.

discrete

(مجزا) - - ویژگی های با ارزش مجزا.

discretized

(گسسته) - - صفت پیوسته است که باید گسسته شود.

ordered

(منظم) - ویژگی های با مقادیر گسسته که باید منظم شود.

cyclical

(ادواری) - ویژگی های با مقادیر گسسته است که منظم و دوره ای است، به عنوان مثال روزهای هفته.

sequence time

(دنباله زمانی) - صفت شامل واحد های اندازه گیری زمان.

sequence

(دنباله) - صفت حاوی کلید مرتب سازی بر صفات مربوطه.

OLE DB-DM

از مدل داده کاوی زیر پشتیبانی می کند

- دسته بندی هنگامی که ویژگی پیش بینی شده ، قطعی است .

- رگرسیون هنگامی که صفت پیش بینی خوشه بندی پیوسته است.

- ارتباط (خلاصه سازی داده ها) شامل قوانین اتحاد.

- ترتیب و تجزیه و تحلیل خطا.

- مدل سازی وابستگی که برای تشخیص وابستگی میان صفات استفاده می شود.

استفاده از OLE DB-DM دو مزیت دارد:

از آنجا که تمام ساختار و محتوای یک DMM ممکن است به عنوان یک رشته XML در

قالب (PMML(Predictive Model Markup Language) بیان شود OLE DB-DM می تواند با

PMML در ارتباط باشد .

OLE DB-DM

می تواند با تکنولوژی OLAP ارتباط داشته باشد
 فن آوری هایی، که در بالا توضیح داده شد مثل XML، PMML، XML-RPC،
 UDDI، SOAP و OLE DB-DM را می توان در ادغام و نیمه خودکار کردن پردازش
 های داده کاوی و کشف دانش در هر دو سطح دستکاری و به اشتراک گذاری داده ها و اطلاعات
 استفاده کرد. مدل فن آوری های مبتنی بر XML را می توان برای ذخیره داده ها و مدل های
 داده کاوی، و ایجاد پروتکل های ارتباطی بین ابزارهای داده کاوی مورد استفاده قرار داد.

OLAP (online analytical processing)

یا (پردازش تحلیلی آنلاین) را میتوان در طول مرحله پردازش داده ها مورد استفاده قرار
 داد، و OLE DB-DM را می توان برای ادغام ابزار داده کاوی با بانکهای اطلاعاتی رابطه
 ای DBMS مورد استفاده قرار داد.

XML

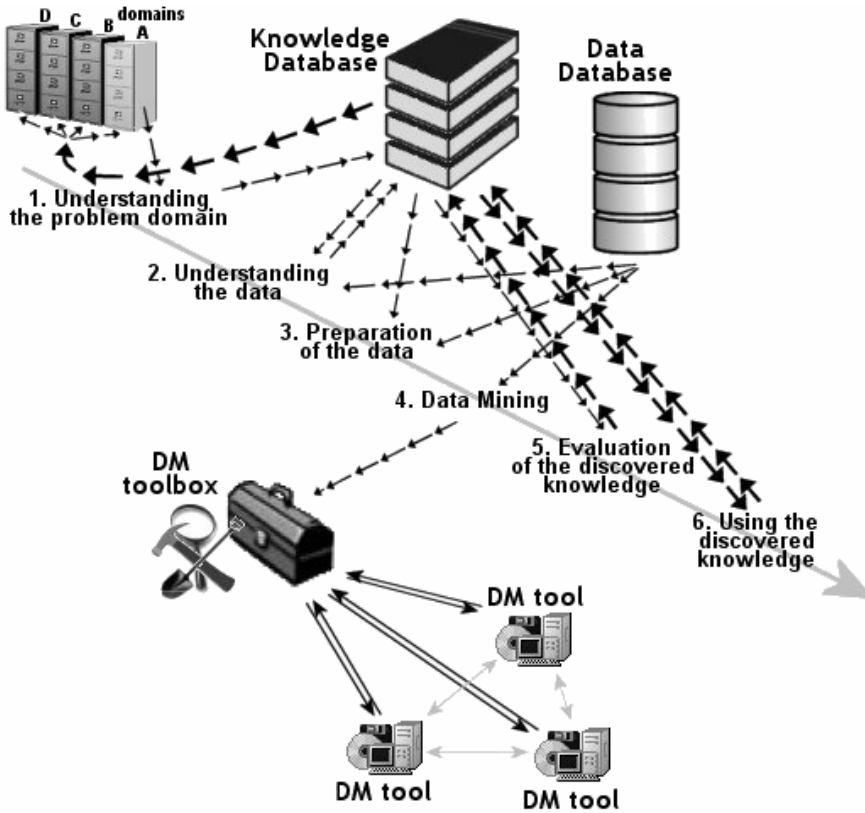
یک فرمت جهانی برای ذخیره سازی داده های ساخت یافته است. از زمانی که توسط
 DBMS ها پشتیبانی شد نه تنها برای انتقال داده بلکه برای ذخیره سازی داده ها به یک
 استاندارد تبدیل شد. از زبان PMML می توان برای انتقال و ذخیره ابر داده استفاده کرد. در واقع
 یکی از فن آوری های است که بطور قابل توجهی می تواند به سادگی در جهت طراحی و تکامل
 سیستم های DMKD همچنین افزایش انعطاف پذیری خود در همان لحظه مورد استفاده قرار
 گیرد. بنابراین ما ساخت مخازن ابر داده (مخازن دانش) که از PMML برای ذخیره محتوای آنها
 استفاده می شود را پیش بینی می کنیم. SOAP و XML-RPC دو پروتکل ارتباطی هستند که
 نه تنها مستقل از پلت فرم است، بلکه هیچ نیازی به فراخوانی مستقیم توابع API هم ندارد،
 ارتباط را آسان می کند، و یک سازگاری کامل بین برنامه های کاربردی که تبادل اطلاعات را
 بعهده دارند را نیز برقرار میکند. آنقدر این پروتکل ها ارتباط ضعیفی دارند، که اگر شخصی
 بخواهد در رابطه با کاربر پسندی آنها صحبت کند می گوید یکی از آنها با ++C و در لینوکس و
 دیگری به زبان کوبول و با سیستم عامل ویندوز نوشته شده است. پروتکل های ارتباطی قدیمی
 که بر پایه مدل های COM، DCOM، CORBA بودند ارتباط تنگاتنگی با هم داشتند که کار

برنامه نویسان را بسیار دشوار ، ناکارآمد و پرهزینه می کرد . پروتکل های ارتباطی SOAP برای پیاده سازی یکپارچگی را به ارمغان آورد چرا که بیشتر بسته های نرم افزاری در حال حاضر کتابخانه هایی از این تکنولوژی را ارائه می کنند . نتیجه اینکه با استفاده از این پروتکل برقراری ارتباط بین ابزارهای داده کاوی و جعبه ابزار داده کاوی بسیار ساده می شود .

UDDI (Universal Description, Discovery and Integration)

به معنی شرح، کشف، و یکپارچه سازی فراگیر فن آوری های کلیدی را قادر به ساخت جعبه ابزارهای داده کاوی انعطاف پذیری می کند، که با استفاده از آن میتوانیم جعبه ابزار آنلاینی که به صورت پویا قادر به جستجو، دسترسی و استفاده از ابزار داده کاوی که خدمات وب را مانند یک وب سرویس منتشر میکند بسازیم OLE DB-DM تکنولوژی است که اجازه استفاده الگوریتم داده کاوی در DBMS ها را بدون از مسائل ارتباط بین ابزار داده کاوی و DBMS ها را میدهد.

ما فکر می کنیم فن آوری های توصیف شده در بالا می توانند برای پشتیبانی از تمام مراحل پردازش DMKD مورد استفاده قرار گیرد شکل ۲ نشان دهنده طراحی مدل DMKD بر اساس پردازش نیمه خودکار DMKD می باشد.

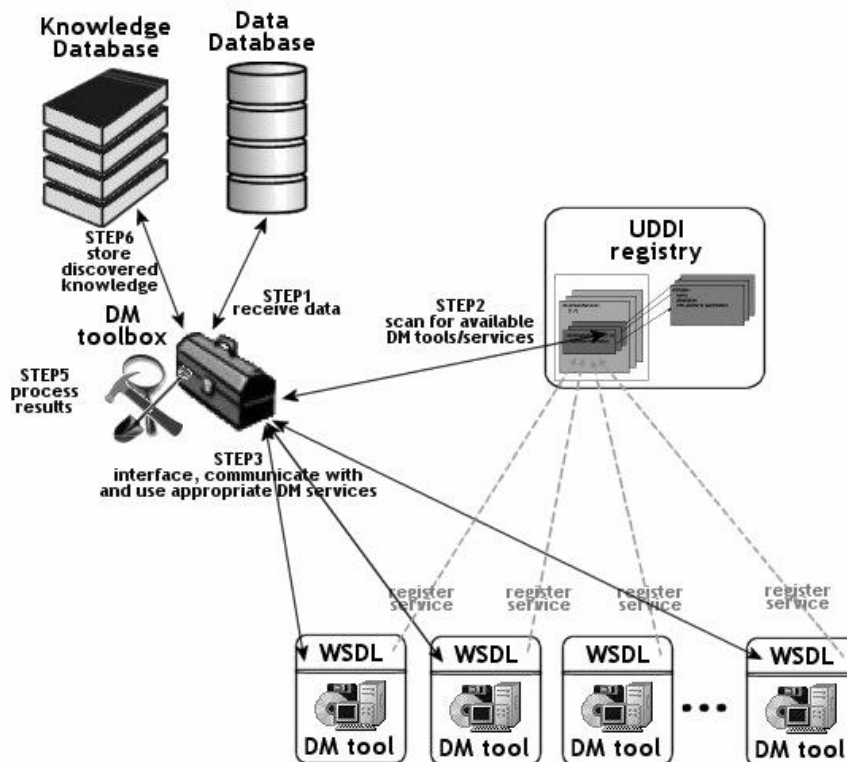


شکل ۲

از آنجائی که PMML از فرمت XML برای ذخیره دانش استفاده می کند ، پایگاه داده و بانک اطلاعاتی دانش را می توان با استفاده از یک DBMS که از XML پشتیبانی می کند ذخیره کرد. داده های پایگاه داده برای ذخیره و پرس و جو داده ه استفاده می شود. با این حال تمام اطلاعات مراحل DMKD، می تواند توسط پایگاه داده دانش ذخیره شود. مزایای استفاده از اجرای پایگاه دانش ذخیره سازی و بازیابی دانش خودکار ، به اشتراک گذاری دانش کشف شده بین حوزه های مختلف و پشتیبانی از دو مرحله DMKD نیمه خودکار است: درک داده ها، و آماده سازی داده ها است. کاملا واضح است که پردازش DMKD بهتر از داده کاوی به تنهایی است .

یک گام داده کاوی ممکن است از یک جعبه ابزار داده کاوی که با چندین ابزار داده کاوی ادغام شده استفاده کند .

در شکل ۳ معماری جعبه ابزار داده کاوی ، که مبتنی برXML است، نشان داده شده است



شکل ۳

ایده پیاده سازی جعبه ابزار داده کاوی ناشی از یک مشاهده ساده که هیچ ابزار داده کاوی به خوبی بر روی تمام انواع اطلاعات اجرا نشده بود نشأت گرفته است. XML و فن آوری های مبتنی بر XML مانند SOAP و UDDI از اجرای چنین جعبه ابزار ساده ای است. جامعه کسب و کار در حال حاضر برای ادغام فرآیند DMKD تلاش می کند. در طی چند سال گذشته بازار کسب و کار نشان داد علاقه رو به رشدی به DMKD دارد. بزرگترین شرکتهای تولیدکننده DMKD مثل IBM، مایکروسافت، اوراکل برخی از ابزار داده کاوی را در سیستم های تجاری خود استفاده می کنند. به دلیل این که استفاده از روش داده کاوی آسان تر است، به ویژه برای کاربرانی که از محصولات DBMS استفاده میکنند.

نتیجه گیری

در حال حاضر صنعت DMKD تخصصی شده است. این صنعت از گروه های پژوهشی تشکیل شده و کارشناسان در این زمینه از نزدیک با تصمیم گیرندگان کار نمی کنند. با وجود اینکه DMKD موقعیتی جهت تولید راه حل های جدید در جامعه ایجاد کرده پیچیدگی و هزینه بالای آن مانعی است برای در دسترس بودن مخاطبان بیشتر. پروژه های DMKD در شرایطی قرار گرفته اند که وجود آنها یک نیاز ضروری است، در حالی که بسیاری از صاحبان مشاغل به دلیل هزینه های بالا از آن صرف نظر می کنند.

فن آوری های شرح داده شده در بالا (XML، XMP-RPC، SOAP، PMML، UDDI،

OLE DB-DM; OLAP

نقش مهمی را در طراحی چارچوب نسلهای بعدی پردازش DMKD دارد. این فن آوری ها ممکن است برای ساخت جعبه ابزار داده کاوی که سرمنشا ابزارهای متعدد داده کاوی برای ساخت مخازن دانش، برقراری ارتباط و تعامل بین ابزارهای DBMS و داده کاوی، مخازن دانش، و از همه مهمتر برای نیمه خودکار کردن تمام پردازشهای DMKD است استفاده شود. این فن آوری ها همچنین می توانند برای گسترش پردازش DMKD که شامل عناصری که بر روی سیستم عامل های مختلف اجرا می شوند و دارای پلت فرم مستقل هستند مورد استفاده قرار گیرد. یکی دیگر از مزایای از این تکنولوژی این است که آنها صنعت DMKD را به سطح جدیدی از قابلیت ها ارتقا می دهد. کاربران جدید، به رغم عدم آگاهی از DMKD، مجذوب برنامه DMKD می شوند.

مضاف بر طراحی و پیاده سازی یک چارچوب جدید DMKD، شاید قبلا فعالیت هائی انجام شده است. مثل طراحی و پیاده سازی نسل جدیدی از سیستم های با کارایی بالای داده کاوی که ترکیب چندین روش داده کاوی هستند، و قادر به استخراج ناهمگن منابع دانش مانند داده های چند رسانه ای، می تواند نتایج را نشان داده و مقادیر عظیمی از داده های پیچیده را بررسی کنند. یکی از اهداف طراحی سیستم ها باید این باشد که طراحی رابط کاربر بهتر شود. نتیجه این کار پذیرش بیشتر محصولات را به دنبال دارد، به خصوص توسط شرکت ها و سازمان های متوسط و کوچک که در آن کاربران ممکن است مهارت های فنی محدودی را داشته

باشند. یکی دیگر از موضوعات بسیار مهم درک کاربر از تازگی، فهم و سادگی دانش تولید شده بوسیله پردازش های DMKD است

منابع:

- [1] داده کاوی و کشف دانش مهدی غضنفری دانشگاه علم و صنعت
- [2] Trends in Data Mining and Knowledge Discovery *Krzysztof J. Cios and
Lukasz A. Kurgan*
- [3] Service-Oriented Data Mining *Derya Birant*
- [4] Bradley, P., Fayyad, U., and Reina, C., Scaling Clustering Algorithms to Large Databases *Proceedings of the 4th International Conference on Knowledge Discovery and Data Mining, Menlo Park, California, pp. 9-15, 1998*
- [5] Cios, K.J., Teresinska, A., Konieczna, S., Potocka, J., Sharma, S., Diagnosing Myocardial Perfusion from PECT Bull's-eye Maps - A Knowledge Discovery Approach *IEEE Engineering in Medicine and Biology Magazine, Special issue on Medical Data Mining and Knowledge Discovery, 19:4, pp. 17-25, 2000*

Abstract

Data Mining and Knowledge Discovery (DMKD) is one of the fast growing computer science fields. Its popularity is caused by an increased demand for tools that help with the analysis and understanding of huge amounts of data. Such data are generated on a daily basis by institutions like banks, insurance companies, retail stores, and on the Internet. This explosion came into being through the ever increasing use of computers, scanners, digital cameras, bar codes, etc. We are in a situation when rich sources of data, stored in databases, warehouses, and other data repositories, are readily available. This in turn causes big interest of business and industrial communities in the field of DMKD. What is needed is a clear and simple methodology for extracting the knowledge that is hidden in the data. In this chapter, an integrated DMKD process model based on the emerging technologies like XML, PMML, SOAP, UDDI, and OLE DB-DM is introduced. These technologies help designing flexible, semi-automated, and easy to use DMKD model. They enable the building of knowledge repositories. They allow for communication between several data mining tools, databases and knowledge repositories. They also enable integration and automation of DMKD tasks

ده حمله برتر به پایگاه داده ها

رضا علیپور

تزریق کدهای SQL (SQL Injection)

ای نوع حمله یک روش تزریق کد SQL می باشد که در آن هکر با استفاده از دستورات SQL در پایگاه داده یک سری فعالیت های غیر مجاز را انجام می دهد این نوع حمله از سال ۲۰۰۷ تا ۲۰۱۰ جزء رایجترین حملات به بانک های اطلاعاتی بوده است.

SQL Injection حمله ایست که در آن به داده های ساکن در پایگاه داده که از طریق فایروال محافظت می شوند حمله می کند این حمله به علت مدیریت ضعیف در اعتبار سنجی کدها و یا ورودی های برنامه (وب سایت) اتفاق می افتد مهاجم از این نوع حمله میتواند در تزریق یکسری از دستورات SQL در یک QUERY با داده های ورودی یک کاربر در یک برنامه مبتنی بر وب خرابکاری ایجاد نماید.

پرس و جو معمولا دارای چند بخش است:

۱. دستور SELECT برای انتخاب ستونهایی از جدول

۲. WHERE برای طراحی یک سری از شروط

۳. FROM برای انتخاب یک ستون از یک جدول خاص

SQL Injection معمولا در بخش where اتفاق می افتد.

یکی از راه های بروز چنین آسیبی عدم فیلتر شدن کارکترهای همچون (" و) می باشد به

عنوان مثال:

```
Statement="select * from users where name ='username';"
```

کد فوق اطلاعات مربوط به یک نام کاربری از جدول users استخراج می کند اما ماجولها می تواند با دادن متغییر دیگری به متغییر username سبب اجرای دستورات متفاوتی شود به عنوان مثال

```
`OR `a`=`a`
```

که کد زیر تولید می شود

```
Select * from user where name=`OR `a`=`a`;
```

یا از روش های زیر استفاده نماید.

```
`OR `a`=`a`--`
```

```
`OR `a`=`a`//`
```

```
`OR `a`=`a`/*`
```

```
Select * from users where name = `OR `a`=`a` --`;
```

با دستورات ذیل سبب حذف جدول userinfo می شود

```
a; DROP TABLE users ;Select * from userinfo where `t`=`t`
```

در سال ۲۰۱۲ گروهی تحت عنوان D33D با نفوذ به زیر دامنه ای از یاهو , yahoo

voices, به همین صورت گواهی نامه های لاگین بیش از ۴۵۰۰۰۰ کاربر را ربودند.

اگر سیستم نرم افزاری پایگاه داده نتواند ورودی ها را پاک کند این حمله می تواند ضربات زیادی به بانک اطلاعاتی بزند روش مقابله با این حمله با استفاده از وصله های امنیتی مداوم است سه روش برای مبارزه با حمله SQL Injection وجود دارد.

۱. جلوگیری از نفوذ(IPS)

۲. کنترل دسترسی به سطح QUEWRY ها(همانند آنچه که در Excessive prissive

Abuse)وجود دارد

۳. ارتباط رویداد

باید ارتباط کاربران خود را از سرور قطع نمود و سپس یک پشتیبان از قفایل های پایگاه داده گرفت . برخی برنامه ها مثل اسکنر Aconelix وجود دارد که ادعا می کند می تواند این حمله را تشخیص دهد که برخی از کمپانی ها و دولت ها نیز از آن استفاده می کنند.

IPS می تواند آسیب های فرآیندهای ذخیره شده و یا رشته های تزریق شده SQL را شناسایی نماید . با این حال IPS به تنهایی در مقابل رشته های تزریق SQL که مبتلا به یک نوع مثبت کاذب هستند قابل اعتماد نیست . اما مدیران امنیتی که فقط بر روی IPS به تنهایی

اتکا کرده‌اند به بمباران تزریق هشدارهی تزریق SQL مواجه می‌شوند. اگرچه با مقایسه یک امضاء تزریق SQL با سایر تجاوزهایی همچون یک حمله کنترل دسترسی سطوح پرس و جو می‌توان با دقت فوق‌العاده‌ای یک حمله واقعی را شناسایی کرد. البته بعید به نظر می‌آید که یک امضاء تزریق SQL و سایر تهاجم‌ها بخواهند یک فرایند تجاری در یک طول طبیعی ظاهر شوند.

پروفایل‌های پویا یک کنترل دسترسی سطح پرس و جو ارائه می‌دهد که بصورت اتوماتیک می‌تواند پروفایل‌هایی را برای هر کاربر یا هر برنامه کاربردی به صورت یک الگوی پرس و جوی نرمال ایجاد کند، که سبب می‌شود هر QUERY که با مقدار مشخص شده الگوهای کاربران یا برنامه‌ها یکسان نباشد فوراً شناسایی گردد.

نمونه‌ای از حمله SQL Injection در ذیل نمایش داده شده است.

```
Exec ctxsys.driloal.validate stmt('grant dba to scott')
```

در این حمله مهاجم (scott) در تلاش است تا امتیاز مدیر پایگاه داده را بوسیله جاسازس

خودش در یک فرایند بدست آورد

نتایج حمله SQL Injection

۱. دسترسی به داده‌های غیر مجاز

۲. دستکاری اطلاعات و داده‌های غیر مجاز

۳. محرومیت از خدمات

۴. ارتقاء امتیاز و اعتبار

حمله تزریق SQL یک حمله جدیدی نمی‌باشد این حمله به سال ۲۰۰۴ بر می‌گردد که در آن زمان ایستگاه تلویزیون آلمان مورد حمله واقع گردید در سال ۲۰۰۶ هکرهای روسی به وب سایت‌های دولتی و اطلاعاتی کارت اعتباری حمله کردند در سال ۲۰۰۸ ده‌ها هزار نفر از طریق وب سایت‌ها و PC های خود و از طریق دستورات SQL مورد حمله واقع شدند.

حمله تخلف امتیاز بیش از حد (Excessive privilege Abuse)

وقتی کاربران و یا برنامه‌های کاربردی امتیازات دسترسی به database را فراتر از نیازهای شغلی و کاری خود اعطا می‌کنند میلیون‌ها هدف مخرب دیگر نیز ممکن است در قبال این امتیاز اضافی بوجود آید. به عنوان مثال یک مدیر دانشگاه که صرفاً وظیفه اش تغییر اطلاعات

شخصی دانشجویان می باشد اگر امتیاز بیش از حد به او تعلق گیرد می تواند تغییرات مربوط به نمرات دانشجو را نیز اعمال نماید.

راه حل مقابله: راه حل مقابله با این حمله حذف تمامی حقوق بیش از حد می باشد که این امر لازمه اش این است که میزان دسترسی هر کاربر به اطلاعات، از قبل تعریف شده باشد و به همان مقدار دسترسی داشته باشد و این محدودیت ها شامل حداقل امکان دسترسی به اعمال دستورات SQL (select و update) و غیره روی اطلاعات می باشد.

ایجاد یک امنیت از طریق مدیریت حقوق کاربران بر روی پایگاه داده (URMD) یک نما و دیدی از حقوق و امتیاز کاربران را بوجود می آورد که می تواند بر روی امتیاز و حقوق هر کاربر تمرکز نماید و آن را تجزیه و تحلیل نماید و داده را با اهمیت را شناسایی نموده تا در مقابله با حملات این چینی واکنش مناسب را نشان دهد. لازم است سازمان ها از عدم اعطای از جحیت و امتیاز به افرادی که در نهایت نقش قرار دارند مطمئن شوند.. به عقیده صاحب نظران به کاربران باید به عنوان بخشی از یک گروه نگریسته شود و به اندازه ای نقشی که در آن گروه دارند حقوق و امتیازات ضروری را از سوی مدیریت به آنان داده شود مدیریت نیز بر امتیازات داده شده بر مبنای نقش به مراتب آسانتر از دادن امتیاز مستقیم به افراد است.

حمله تخلف امتیاز مشروع (Legitimate privilege Abuse)

امکان این که کاربران از امتیاز قانونی و مشروع خود در جهت مقاصد غیر مجاز استفاده کنند وجود دارد . به عنوان مثال یک کارمند بهداشت را در نظر بگیرید که این فرد می تواند به تاریخچه پزشکی یک بیمار بصورت قانونی دسترسی داشته باشد اما می تواند از این اطلاعات در جهت غیر مجازی استفاده نماید مثلا می تواند آن را بمنظور کسب پول از طریق فروش پرونده های پزشکی به افراد ناشایست استفاده نماید.

راه حل مقابله با حمله امتیاز مشروع , کنترل دسترسی به پایگاه داده است .

نتایج حمله امتیاز مشروع:

۱. از دست رفتن داده ها
۲. سرقت اطلاعات
۳. اختلاس

حمله افزایش امتیاز (privilege elevation)

تعریف: استفاده کاربر سطح پایین از اطلاعات سطح بالای پایگاه داده

انواع آسیب‌ها:

- سرریز بافر
- تزریق SQL
- اشکالات معنایی

یکی از آسیب‌های بسیار شایع در پایگاه داده امکان افزایش میزان ارجحیت توسط مهاجمان با استفاده از حساب کاربری دارای حق ارجحیت پایین و دستیابی به حق ارجحیت مدیر سیستم است برای نمونه می‌توان سوء استفاده یک مهاجم را از یک تابع که در SYSDBA اجرا می‌شود را نام برد تا وقتی که این آسیب پذیری وجود داشته باشد مدیران سیستم ناچار به اداره کردن آنها یا بکارگیری وصله‌های امنیتی و بروز کردن‌های سروقت خواهد بود البته مهاجمان می‌توانند از طریق آسیب‌پذیری‌های نرم افزاری پلت فرم پایگاه داده به این حق دسترسی پیدا کنند این آسیب‌پذیری‌ها می‌تواند در روش ذخیره شدن داده‌ها، توابع، پیاده‌سازی پروتکل‌ها و حتی SQL نمایان شود

برای مثال یک شرکت نرم‌افزاری در یک موسسه مالی ممکن است از یک تابع خاص برای بدست آوردن امتیاز دسترسی به پایگاه داده استفاده کند و از این طریق یک حساب جعلی درست نماید و وجوه مختلف را در آن جابجا نماید

راه حل:

این حمله را می‌توان از طریق ترکیبی از سیستم جلوگیری از نفوذ سنتی IPS و کنترل دسترسی در پرس و جوها کنترل نمود. IPS ترافیک پایگاه داده را بازرسی می‌کند تا الگوهایی که مربوط به آسیب‌پذیری هستند را شناسایی کند. برای نمونه اگر یک تابع به عنوان یک وخطر شناخته شود IPS تمامی دسترسی‌ها به این تابع را مسدود می‌کند یا در صورت امکان آن را بلوکه می‌نماید. متأسفانه تمامی این حملات توسط IPS به تنهایی قابل تشخیص نیست چون بسیاری از توابع پایگاه داده به طور معمول برای مقاصد قانونی است بنابراین مسدود کردن همه آنها امکان‌پذیر نمی‌باشد. IPS باید به دقت نقاط و توابع آسیب‌پذیر را جدا نماید. IPS ممکن است بمنظور چک کردن اینکه آیا یک تابع می‌تواند درخواستی از پایگاه داده داشته باشد را بر

عهده گیرد ولی در کنترل دسترسی پرس و جو بمنظور تشخیص مکانیزم رفتار کاربران عادی می باشد.

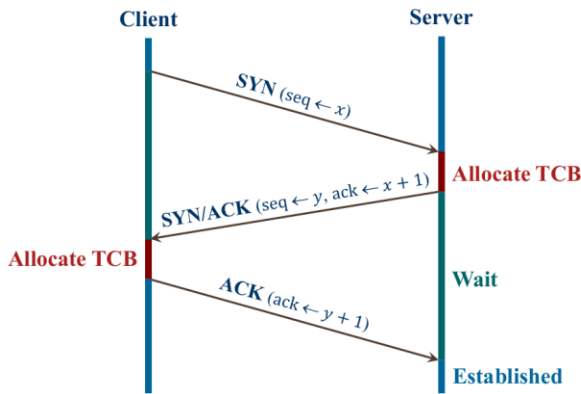
حمله انسداد سرویس (Denial of service)

هدف از حمله dos جلوگیری از دسترسی مجاز کاربران قانونی به منابع یک سیستم یا ایجاد تاخیر در عملیات آن سیستم می باشد. روش های حمله:

- سوء استفاده از عیوب موجود در پیاده سازی یا پیکر بندی یک سرویس خاص
- سوء استفاده از ویژگی ها یا نقاط ضعف موجود در طراحی یک پروتکل خاص
- مصرف منابع

- پهنای باند
- حافظه
- Cpu

مثال:



- Syn flood
- Udp flood
- Icmp flood
- Smurf
- Fragggle
- Teardrop
- Land
- Ping pf death

SQL slammer تصویر روشنی از توانایی هکر ها در استفاده از آسیب پذیری DBMS در از کار انداختن سرورهای پایگاه داده از طریق ایجاد سیل ترافیکی ارائه می دهد نکته جالب و واضح قضیه این است که وقتی SQL slammer در سال ۲۰۰۳ هویدا شده بود یک وصله امنیتی برای مقابله با این کرم از قبل آماده شده بود حتی پس از هفت سال sql slammer هنوز به آزارهای خود ادامه می دهد و سرورهایی که از وصله های امنیتی استفاده نکرده اند را مورد قرار می دهد. sql slammer نوعی کرم رایانه ای است که سبب بروز خطای denial of service در

برخی از میزبان‌ها شده و در زمان سرایت آلودگی به طرز چشمگیری سرعت کل اینترنت در جهان کاهش داده شد.

این کرم در تاریخ ۲۵ ژانویه ۲۰۰۳ کار خود را آغاز کرد و در کمتر از ۱۰ دقیقه ۷۵۰۰۰ رایانه را آلوده کرد بسیار روشن است وقتی آلودگی slammer در سال ۲۰۰۳ راه افتاد یک پیچ وجود داشت که آن آسیب‌پذیری را و نحوه مقابله با آن را مورد پوشش قرار داد.

DOS یک دسته حمله عمومی است که برای دسترسی به برنامه‌های کاربردی شبکه و یا داده‌ها که برای کاربران در نظر گرفته شده است طراحی شده است. DOS ممکن است از طریق بسیاری از تکنیک‌های مربوط به آسیب‌پذیرهایی که قبلاً توضیح داده شد بوجود آید. به عنوان مثال DOS می‌تواند با استفاده از بدست آوردن مزایای یک پایگاه داده آسیب‌پذیر یک سرور را به سقوط بکشاند. تکنیک‌های دیگر DOS شامل فساد داده‌ها، سیل شبکه و استفاده بیش از حد از منابع سرور (حافظه، سرور و غیره) می‌باشد. DOS اغلب مرتبط با یک کلاه برداری و اخاذی یک مهاجم از راه دور است که در آن بارها و بارها تا مرز قربانی شدن یک سرور و یا وجوه سپرده حساب بانکی بین‌المللی پیش می‌رود. هر DOS نشان‌دهنده یک تهدید جدی برای یک سازمان است.

راه مقابله:

جلوگیری و ممانعت از DOS نیازمند یک پشتیبانی در سطوح مختلف است. حمایت در سطح شبکه، نرم‌افزار و پایگاه داده یک امر ضروری است. کنترل اتصال مانع استفاده بیش از حد از اتصال، میزان پرس و جو و متغیرهای دیگر برای هر کاربرد در پایگاه داده می‌شود. IPS و پروتکل اعتبارسنجی روش دیگری برای جلوگیری از بهره‌برداری DOS از آسیب‌های نرم‌افزاری شناخته شده می‌باشد از طرفی دیگر پروفایل‌های پویا یک کنترل دسترسی پرس و جو را برای شناسایی هرگونه تغییر ایجاد می‌کنند. در زمانبندی پاسخ یک حمله DOS منجر به تاخیر در پایگاه داده و جوابدهی می‌شود و با این ابزار می‌تواند تاخیر بیش از حد را تشخیص داد و جلوی آن را گرفت.

حمله از طریق آسیب پذیری در بسترهای نرم افزاری پایگاه داده (database platform vulnerabilities)

آسیب پذیری در سیستم عامل ها ممکن است باعث ایجاد دسترسی به اطلاعات غیر مجاز و فساد گردد. به عنوان مثال کرم بلستر با استفاده از آسیب پذیری win2000 توانست به سرور هدف حمله نماید

راه مقابله:

IPS یک ابزار نسبتاً خوبی برای شناسایی و بلاک کردن حملات طراحی شده از طریق آسیب پذیری بسترهای نرم افزاری می باشد. منظور از بستر، نرم افزار، شبکه، سیستم عامل، پایگاه داده و سخت افزار و نرم افزارهای مرتبط می باشد. امنیت در هر یک از حوزه ها باید جداگانه مورد بررسی قرار گیرد ولی از لحاظ تعامل با نرم افزار نیز باید نکات امنیتی را لحاظ کرد. در واقع نرم افزار بایستی بصورت مستقل عمل نماید. برای استقلال نرم افزار باید تمامی پروتکل ها و تعاملات نرم افزار باید بصورت استاندارد پیاده سازی شده باشد.

اثرات این حمله:

- به خطر افتادن سرور
- دسترسی مستقیم به فایل های پایگاه داده
- دسترسی محلی از طریق نقش های مدیر

حمله تایید ضعیف (weak Authentiction)

ممکن است در یک سازمان بزرگ صدها و یا هزاران پایگاه داده وظیفه طاق فرسای دلهره آور باشد اما از بین بردن نام کاربری و رمز ورود به سیستم که هنوز در حالت پیش فرض، خالی یا از نظر امنیتی ضعیف هست بسیار دشوار می باشد.

افراد نفوذ گر همواره در گام اول نفوذ به دنبال پیگیری حساب هایی هستند که نام کاربری و رمز عبور پیش فرض دارند و هر زمانی که این امکان برایشان میسر شود لحظه ای در نفوذ به سیستم تردید نخواهند کرد

راه مقابله:

استفاده از ۲ فاکتور تایید هویت

- اجرای سیاست رمز عبور قوی
- شناسایی حمله
- اطمینان از اینکه کاربران کلمات عبور قوی را انتخاب کردخ اند
- اطمینان از مکانیزم احراز هویت برای امنیت قوی پیکر بندی

بعنوان مثال سیستم عامل unix معمولاً به صورت رمز شده در یک فایل می باشد که می توان آن را توسط یک کاربر عادی بخواند و براحتی می توان رمز عبور آن را به سادگی کپی و یا از طریق تعدادی از روش های دیگر بدست آورد. زمانیکه محتویات یک پرونده توسط هکر رمز گشایی گردید براحتی می تواند داخل سیستم نفوذ نموده و عملیات تخریب را انجام دهد. کلمه عبوری که کمتر از ۸ کارکتر باشد و فقط کلمات انگلیسی باشد یک کلمه عبور ضعیف شمرده می شود

حمله به نسخه پشتیبان (Backup database exposure)

موارد متعددی از نقض های امنیتی مربوط به سرقت از نسخه پشتیبان بانک اطلاعاتی وجود دارد پشتیبان گیری از پایگاه داده یک ابزار ذخیره سازمان می باشد به طور کامل متاسفانه محافظت نشده است.

راه مقابله:

رمز نگاری کردن اطلاعات پشتیبان گرفته شده برخی از فروشندگان نیز پیشنهاد داده اند که در آینده محصولات DBMS امکان پشتیبان گیری تکه ای نداشته باشند. در IT یک backup و یک فرایند backup گیری و یا آرشیوی از اطلاعات کامپیوتری ارجاع می شود که می تواند در مواردی که اطلاعات ما از بین رفت بازخوانی شود

Backup هدف های ذیل را دنبال می کند:

- بازگرداندن اطلاعات از دست رفته
- جایگزین مناسبی برای داده های مورد حمله واقع شده

از آنجایی که یک سیستم پشتیبان , حداقل یک کپی از تمام داده های با ارزش است پس نیاز به یک فضای مناسبی دارد. سازماندهی در این فضای ذخیره سازی و مدیریت فرایند پشتیبان می تواند امری پیچیده باشد. امروزه مدل های مختلفی برای ذخیره سازی اطلاعات

وجود دارد قبل از اینکه داده ها به محل ذخیره سازی فرستاده شوند ممکن است مورد حمله و دستکاری قرار گیرند . تکنیک های بسیاری برای بهینه سازی برای مواجهه با فایل های باز و منابع داده زنده و همچنین فشرده سازی، رمز گذاری و غیره می باشد. در پشتیبان گیری باید اطمینان از صحت اطلاعات پشتیبان گیری شده وجود داشته باشد.

حمله به واسطه آسیب پذیری پروتکل های پایگاه داده

(Database protocol vulnerabilities)

تعداد فزاینده ای از آسیب پذیری ها امنیتی هستند که در پروتکل های ارتباطی پایگاه داده شناخته شده اند مثلا کرم sql slammer با استفاده از عیب در پروتکل میکروسافت sql سرور توانست شرایط DOS را بوجود آورد. همواره باید یک اسکن امنیتی بصورت دوره ای از پایگاه داده انجام داد چون محیط همواره در حال تغییر است.

در این حمله از خصوصیات یا خطای پیاده سازی تعدادی پروتکل که در ماشین قربانی نصب شده برای مصرف میزان اضافی منابع آن استفاده می شود برای مثال حمله TCP SYN از ضعف ذاتی قانده دست تکانی سه مرحله ای در ارتباط با TCP استفاده می کند.

سرور به محض دریافت درخواست SYN اولیه از طرف متقاضی ارتباط وابسته SYN/ACK را به او برگردانده و منتظر ACK حمله سیلابی بسته SYN را ترتیب می دهد سرور به این بسته ها پاسخ داده و منتظر ACK از طرف متقاضی ارتباط می ماند در حالیکه این ACK اصلا وجود ندارد . از آنجایی که سرور فضای محدودی برای ارتباطش دارد بدلیل سرریز بفر سرور دیگری قادر به پردازش ارتباطات ورودی نیست حملات PUSH ACK, CGI مثال هایی دیگر از این نوع حملات هستند.

این نوع حمله به علت پیکر بندی ضعیف سرورهای وب اتفاق می افتد و باعث حملات بسیار خطرناک می شود شاید هنوز هیچ کس حملات یونیکد و رمزگشایی را فراموش نکرده باشد که این مشت نمونه خروار این گونه حملات است اما آنچه که می خواهیم بیان کنیم این است که دیواره آتش نمی تواند در این نوع حمله از سرور دفاع کند که این نوع حمله از طریق پروتکل HTTP و از طریق پورت ۸۰ یا ۴۴۳ انجام می شود.

حمله از طریق کپی برداری غیر مجاز از اطلاعات حساس

(Unauthorized copies of sensitive pak)

بسیاری از شرکت‌ها در تلاش برای پیدا کردن راهی برای حفاظت و دقت موجودی پایگاه داده خود هستند یک پایگاه داده جدید ممکن است بدون در نظر گرفتن هیچگونه امنیتی و بدون در نظر گرفتن حساسیت داده‌های خویش در معرض خطر حمله قرار گیرد این پایگاه داده ممکن است شامل اطلاعاتی همچون جزئیات معامله مشتری کارمند باشد و بدون علم داشتن به حساب داده‌ها، کنترل سخت خواهد بود و این واقعیت وجود دارد که این اطلاعات حساس ممکن است به طور غیر قانونی در دسترس توسط کاربران یا هکرها باشد.

راه مقابله:

بمنظور حفظ موجودی دقیق پایگاه داده سازمان می‌بایست تمامی اطلاعات حساس بر روی پایگاه داده شناسایی شود مرحله بعد طبقه بندی این اطلاعات حساس می‌باشد. در این مورد معمولاً مهاجمان سعی در کپی برداری و یا سرقت اطلاعات می‌نمایند. که دارای طبقه بندی اطلاعاتی است با عنایت به اینکه غالب مراکز استراتژیک و سازمان‌ها اقدام به مکانیزه نمودن فرایند نگهداری از اسناد و مدارک و انجام امور اداره و روزانه خود نموده‌اند لذا معمولاً باید لایه‌های دسترسی گوناگون امکان استفاده از بانک‌های اطلاعاتی را برای مدیران و یا افراد مجاز مهیا نموده‌اند لذا خطر حضور و نفوذ مهاجمان و در پی آن خطر سرقت اطلاعات و کپی برداری از آنها همواره نگران‌کننده خواهد بود

در حقیقت مهاجمین با استفاده از دسترسی کاربران مجاز و با دسترسی به کدهای آنها به اطلاعات طبقه بندی شده و با ارزش دست یافته و بدین وسیله اقدام به سرقت اطلاعات می‌نمایند.

منابع:

- www.imperva.com
 - database attacks,james bleeker
 - injection database from wikipedia
 - www.bcs.org
 - denial of service,lee grabber
 - J. Mirkovic, S. Dietrich, D. Dittrich, and P . Reiher , Internet
 - Denial of Service: Attack and Defense Mechanisms, Pren-tice Hall, .۲۰۰۴
- جزوه امنیت شبکه دکتر مهدی آبادی

امنیت اطلاعات در آرشیو الکترونیکی اسناد هویتی ایرانیان

فاطمه بابایی^۱، مهدی جمالی^۲

چکیده:

بحث امنیت اطلاعات در سازمان هایی که از آرشیوهای الکترونیکی استفاده می کنند بسیار با اهمیت است. تامین امنیت شبکه و زیرساخت ها، تامین امنیت برنامه های کاربردی و پایگاه داده ها، تست امنیت، حفاظت اطلاعات و مدیریت سیستم های اطلاعاتی از جمله مباحثی است که باید در این حیطه به آنها پرداخته شود. این مقاله یک دید کلی از امنیت اطلاعات و مفاهیم اصلی آن فراهم می کند.

یافته ها

براساس پژوهش حاصل، کانون توجه استراتژی های به کار گرفته شده در زمینه مدیریت اسناد هویتی، تامین امنیت اطلاعات محرمانه است. در واقع این استراتژی ها هدف استفاده از فناوری نوین در خدمات الکترونیک و افزایش امنیت اطلاعات را دنبال می کنند. تمام ادارات تحت نظارت یک سازمان باید از برنامه های یکپارچه ای برای مدیریت اطلاعات هویت الکترونیکی استفاده کنند.

نتیجه گیری

اگرچه رسیدن به دولت الکترونیک و نحوه ارائه خدمات دولتی به تصمیمات سازمان وابسته است، اما به نظر می رسد قدم برداشتن در این حیطه نیازمند زیربناهایی می باشد که همان اصلی برنامه خدمات الکترونیک دولت را دربر بگیرد، امنیت بالاتر شبکه در سازمان تنها به داشتن یک دیواره آتش ختم نمی شود بلکه برای دستیابی به این مقوله بسیار مهم باید به طور دقیق مشخص شود که چه اطلاعاتی باید مورد مدیریت و تامین امنیت قرار بگیرند.

کلمات کلیدی: آرشیو الکترونیکی، امنیت اطلاعات، اسناد هویت ایرانیان، جامعیت اطلاعات، الگوهای سازمانی

^۱ - کارشناس امور پردازش اطلاعات ثبت احوال قزوین، دانشجوی کارشناسی ارشد فناوری اطلاعات دانشگاه آزاد

Fatemebabayi@yahoo.com قزوین

^۲ - معاونت امور اسناد هویتی اداره ثبت احوال قزوین

مقدمه

بدلیل افزایش روز افزون اسناد الکترونیکی در سازمان و لزوم نگه داری و مدیریت این اسناد استفاده از سیستم های مدیریت اطلاعات و نرم افزار های امنیتی مطمئن یک ضرورت به شمار می آید. به گونه ای که حفظ تعداد زیادی از این اسناد در کنار یکدیگر جهت دسترسی کاربران در سطوح مختلف در سراسر کشور را میسر سازد. لازمه نیل به این هدف مهم نویسنده این مقاله را برآن داشت تا ضمن بررسی چگونگی آرشیو اسناد الکترونیکی به دوچالش پیش روی آن بپردازد.

اولین چالشی که در آرشیو اسناد الکترونیکی مدنظر قرار می گیرد امنیت و حفظ اطلاعات محرمانه اسناد است، تامین امنیت در فضای تبادل اطلاعات سازمانها، دفعتا مقدور نمی باشد و لازم است این امر بصورت مداوم در یک چرخه ایمن سازی شامل مراحل طراحی، پیاده سازی، ارزیابی و اصلاح، انجام گیرد.

چالش دوم نیاز به طراحی سیستم های الکترونیکی به گونه ای است که بتواند اطلاعات جدید هر فرد به سوابق گذشته اضافه نماید به گونه ای که جامعیت اطلاعات جدید و گذشته حفظ گردد.

در مقاله حاضر جوانب یاد شده در آرشیو الکترونیکی اسناد از نقطه نظر الگوی سازمانی بررسی گردیده است.

اهمیت امنیت اطلاعات

هدف از امنیت اطلاعات، استفاده از مجموعه ای از سیاستها، راهکارها، ابزارها، سخت افزارها و نرم افزارها، برای فراهم آوردن محیطی عاری از تهدید در تولید، پالایش، انتقال و توزیع اطلاعات در آرشیوهای الکترونیکی است. فراهم آوردن چنین محیطی مستلزم انجام مواردی است که می توان از آنها به عنوان نیازهای امنیتی اطلاعات نام برد که برخی از این موارد در زیر ذکر شده اند:

- ارزش هر سند آرشیو شده برای مالک آن مشخص است و حفظ مندرجات آن مسئولیتی بدیهی برای سازمان به شمار می آید.
- تمهیدات لازم اعم از سخت افزاری و نرم افزاری برای حفاظت از اطلاعات باید فراهم شود.

- سیاستگذاری یکپارچه و سازگار در خصوص امنیت اطلاعات در بخشهای مختلف مدیریتی یک سازمان اعمال شود.
- سازوکار و تشکیلات مناسب جهت تطبیق امنیت اطلاعات با پیشرفتهای تکنولوژی تولید ، توزیع و انتقال اطلاعات از یک طرف و تهدیدات جدید از طرف دیگر فراهم شود.
- امنیت اطلاعات مانع و محدودیتی برای دسترسی کاربران مجاز آن فراهم نکند.
- امکان تعقیب عملکردهای مشکوک روی اطلاعات فراهم شده باشد (Halas,2008,page 3-4).

عوامل موثر در طراحی سیستم مدیریت امنیت اطلاعات

- ۱) نیازمندیهای امنیتی: سازمان باید با توجه به محرمانه بودن اطلاعات فردی و به منظور جلوگیری از خطرات جعل اسناد هویتی از مندرجات آن به نحوی مناسب محافظت کند. با توجه سطوح حساسیت امنیتی اطلاعات هویتی ایرانیان باید راه حل ثابتی برای سازمان در نظر گرفته شود تا ضمن حفظ وحدت رویه کلیه ادارت امنیت لازم را فراهم نمایند.
- ۲) رویکرد مورد نظر در سازمان: برای پیاده سازی سیستمهای مدیریت امنیت، روشها و الگوهای گوناگون فنی و مدیریتی پیشنهاد شده است ، یکی از این روشها رویکرد فرایند محور است . امنیت اطلاعات در یک سازمان به یکباره حاصل نمی شود و در واقع امنیت یک فرایند تکاملی و تدریجی است .
- ۳) اندازه و ساختار سازمان: امنیت اطلاعات یک هدف مدیریتی و بخشی از ساختار مدیریتی سازمان است. با توجه گسترش فعالیت های سازمان و توزیع اسناد هویتی در سراسر کشور به نظر میرسد راه اندازی و راهبری یک سیستم مدیریتی در آن پیچیده تر خواهد بود. مطالعات نشان داده است که هزینه، زمان و کارکنان بیشتری در یک سازمان بزرگ برای پیاده سازی امنیت نیاز است (Asogwa,2012,page 5-7).

رویه های راه اندازی سیستم مدیریت امنیت اطلاعات

با توجه به رویکرد فرایند محور، کلیه راه حل های ارائه شده باید طی مراحل چهارگانه طراحی، پیاده سازی (اجرا)، ارزیابی و اصلاح به صورت یک چرخه همیشگی و ادامه دار در کلیه راه حل های امنیتی اعم از فنی و مدیریتی اعمال شود.

چرخه سیستم مدیریت امنیت اطلاعات

الف (طراحی

استقرار سیستم مدیریت اطلاعات شامل تعیین خط مشی ها، اهداف، فرایندها و روالها به منظور مدیریت مخاطرات در راستای اهداف سازمان است. در این مرحله، باید سرمایه اولیه راه اندازی سیستم، روشهای مستند سازی، رویکرد مدیریت مخاطرات و نیز روشهای اختصاص منابع مشخص شود. در واقع باید اطمینان حاصل شود که محتوا و محدوده اطلاعات سازمانی به طور دقیق و مناسب مشخص شده است (Asogwa, 2012, page 9).

فعالیت‌های مورد نیاز در این مرحله عبارت‌اند از:

(۱) تعریف محدوده مدیریتی: اولین قدم تعیین محدوده و میدانی است که نیاز است تا امنیت در آن در نظر گرفته شود و هدف سیستم مدیریت امنیت اطلاعات است. قلمرو مدیریت آرشيو الكترونيكي در سازمان با توجه به دارایی‌ها و فناوری‌های سازمان مشخص می شود (Australasia Archives council, 2006, page 13).

(۲) تعریف خط مشی های مدیریتی: سیاست یا خط مشی امنیت در تمام فرایندهای مدیریت اطلاعات و به تبع آن تامین امنیت اطلاعات یک نقش کلیدی ایفا می کند، به طوری که در تمام تجربیات موفق مدیریت امنیت، سند خط مشی به عنوان شالوده، مبنا و نقطه آغاز یک طرح مدیریت امنیت موفق برشمرده شده است. هدف هر خط مشی در واقع تعریف و تأثیرگذاری بر تمامی رفتارها، عملکردها و تصمیم گیری‌هاست، به گونه‌ای که مشخص شود چه چیزی برای کاربران مجاز و چه چیزی غیرمجاز است (Australasia Archives council, 2006, page 14).

(۳) تعیین مخاطرات: در این مرحله باید مخاطرات موجود را شناسایی کرد. بدین منظور ابتدا شناخت سرمایه ها و صاحبان آنها در قلمروسازمان ضروری است. سپس باید تهدیدهای متناظر با اسنادهویی را مشخص کرد. تعیین آسیب پذیری‌ها و عواقب تهدیدها در مرحله پایانی این فاز قرار دارد.

(۴) ارزیابی مخاطرات: اساس کارسیستم های مدیریتی، مدیریت مخاطرات امنیتی است. یکی از مهمترین قابلیت‌های سیستم های مدیریت اطلاعات "مدیریت ریسک" است. مدیریت ریسک مجموعه فعالیت‌های طرح ریزی، ارزیابی و کنترل مبتنی بر نتایج تحلیل ریسک است.

ریسک یا مخاطره عبارت است از احتمال ضرر و زبانی که متوجه یک دارایی سازمان مانند سخت افزار ، نرم افزار، اطلاعات ، ارتباطات ، کاربران و ... است. عدم قطعیت در نتیجه مقیاس ناپذیری یکی از مهمترین ویژگیهای مفهوم ریسک است. لذا این عدم قطعیت به معنای غیر قابل محاسبه و مقیاس بودن ریسکها نیست.

برای تحلیل مخاطرات وارد بر سیستم اطلاعات، باید ابتدا مخاطرات را تعیین کرد و ارزش هر مخاطره را تخمین زد.

تحلیل ریسک شامل سه فرایند زیر است:

- تعیین لیست مخاطرات موجود؛

- تخمین نرخ بروز مخاطرات و تخصیص مقدار ارزشی (عددی، کیفیتی و...);

- ارزیابی مخاطرات بر مبنای ارزش مخاطره، احتمال رخداد و عواقب آن.

نتیجه این عملیات، تعیین ریسکهای موجود در سازمان خواهد بود که عملکرد سازمان را تحت تاثیر قرار میدهند و اهداف سازمان را تخریب می کنند.

۵) انتخاب کنترل های مناسب: بر اساس نتایج حاصله از ارزیابی مخاطرات، کنترل های مناسب برای آنها برگزیده می شود. در سیستم های مدیریت اطلاعات صرف نظر از رویکرد انتخابی در طرح ارزیابی مخاطرات، آنچه که اهمیت دارد، وجود این طرح و اجرای صحیح آن است. خروجی اصلی فرایند مدیریت ریسک، سندی حاوی لیست کنترل های مورد نظر و اهداف هر کنترل است که «بیانیه کاربرد» شناخته می شود (Australasia Archives council,2006,page17).

ب) اجرا

در این بخش باید کلیه کنترل ها، عملیاتی و پیاده سازی شوند. نیاز به رویه های جهت تشخیص سریع و پاسخگویی به حوادث، وجود دارد. همچنین کلیه کارمندان و افراد سازمان باید نسبت به امنیت در سازمان، آگاهی لازم را داشته باشند و دوره های آموزشی لازم جهت عملکرد مناسب برای برخورد با ریسک و تهدید را بگذرانند. فعالیتهای این مرحله عبارت است از :

- فرموله کردن طرح برخورد با مخاطرات؛

- اجرای طرح برخورد با مخاطرات؛

- پیاده سازی کنترل‌های امنیتی انتخاب شده؛
- اجرای برنامه های آموزش و آگاهی‌رسانی؛
- مدیریت منابع و فعالیتها.

تعیین سیاستهای امنیتی و اعمال آن ها در سازمان نیز باید در این مرحله انجام شود. یک سیاست امنیتی در واقع انجام اعمالی است که باید صورت گیرد تا بتواند از اطلاعات ذخیره شده در کامپیوتر محافظت کند. یک سیاست امنیتی موثر باعث ایجاد امنیت نسبی برای کاربران می شود که در واقع یک استراتژی برای نگهداری اطلاعات و منابع شبکه است.

ج) ارزیابی

هدف از این مرحله، حصول اطمینان از اجرای به موقع کنترل‌های امنیتی و برآورده شدن اهدافی است که به دنبال دارند. ارزیابی میزان کارایی و تاثیر سیستم‌های مدیریت اطلاعات در این مرحله انجام می‌گیرد. اجرای روال‌های ارزیابی، مرور فرایندها و خط‌مشی‌ها، انجام بازرسیهای دوره‌ای درون سازمانی و برون سازمانی از آن جمله است. فعالیتهای کنترلی متنوعی وجود دارد، اما بازرسیهای داخلی سیستم های اطلاعاتی و مدیریت بازمینی از مراحل اجباری برای پیاده سازی امنیت در سازمان‌اند. پس از پیاده سازی سیاستهای امنیتی، با استفاده از سیستم‌های تشخیص نفوذی، یا سیستم‌های واقعه نگاری، کلیه دسترسی‌های غیر مجاز به شبکه و عبور از سیستم‌های امنیتی مشخص و در فایل های ثبت وقایع خروجی، ذخیره می‌شود. سپس با استفاده از ابزار امنیتی، کلیه پورت‌ها و سرویس‌های شبکه و یا محل‌های نفوذ به شبکه بازرسی می شوند و اطلاعات مربوطه در فایل ثبت وقایع قرار می گیرند. همچنین در این قسمت با استفاده از یکسری ابزار، به تحلیل فایل‌های ثبت وقایع و اطلاعات پرداخته می شود و نتایج حاصل از آنها، جهت بهبود عملکرد سیستم امنیتی شبکه، استفاده و سپس در سیاستهای امنیتی شبکه اعمال می شود.

د) اصلاح

بر اساس نتایج مرحله ارزیابی می‌توان اقدامات اصلاحی را در جهت بهبود عملیات مدیریتی و تامین امنیت به انجام رساند. این اقدامات را می‌توان در دو مقوله طبقه بندی کرد:

۱) در زمان تعامل فناوری با اطلاعات، عکس العمل لازم در برابر یک مشکل امنیتی می تواند از نوع پیشگیرانه (کنشی) یا اصلاحی (واکنشی) باشد. پس از تحلیل مخاطرات، باید اقدامات دفاعی اتخاذ و کنترل های مناسب بر آنها اعمال شود.

۲) بر اساس سطوح پیاده سازی نظام های امنیتی در یک محیط دیجیتال، فناوری امنیت اطلاعات (صرف نظر از نوع واکنشی یا نوع کنشی) در سه سطح، شبکه، میزبان و برنامه های کاربردی، پیاده سازی می شود.

مدیریت امنیت اطلاعات و استانداردهای آن

با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش سیستماتیک به مقوله ایمن سازی فضای تبادل اطلاعات شکل گرفت. بر اساس این نگرش، تامین امنیت فضای تبادل اطلاعات سازمانها، دفعتا مقدور نمی باشد و لازم است این امر بصورت مداوم در یک چرخه ایمن سازی شامل مراحل طراحی، پیاده سازی، ارزیابی و اصلاح، انجام گیرد. برای این منظور لازم است هر سازمان بر اساس یک متدولوژی مشخص، اقدامات زیر را انجام دهد:

۱- تهیه طرح ها و برنامه های امنیتی مورد نیاز سازمان

۲- ایجاد تشکیلات مورد نیاز جهت ایجاد و تداوم امنیت فضای تبادل اطلاعات سازمان

۳- اجرای طرح ها و برنامه های امنیتی سازمان

در حال حاضر، مجموعه ای از استانداردهای مدیریتی و فنی ایمن سازی فضای تبادل اطلاعات سازمانها ارائه شده اند که استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس، استاندارد مدیریتی ISO/IEC 17799 موسسه بین المللی استاندارد و گزارش فنی ISO/IEC TR 13335 موسسه بین المللی استاندارد از برجسته ترین استانداردها و راهنماهای فنی در این زمینه محسوب می گردند.

در این استانداردها، نکات زیر مورد توجه قرار گرفته شده است:

۱- تعیین مراحل ایمن سازی و نحوه شکل گیری چرخه امنیت اطلاعات و ارتباطات سازمان

۲- جزییات مراحل ایمن سازی و تکنیکهای فنی مورد استفاده در هر مرحله

۳- لیست و محتوای طرح ها و برنامه های امنیتی مورد نیاز سازمان

۴- ضرورت و جزییات ایجاد تشکیلات سیاستگذاری، اجرائی و فنی تامین امنیت اطلاعات

و ارتباطات سازمان

۵- کنترل‌های امنیتی موردنیاز برای هر یک از سیستم‌های اطلاعاتی و ارتباطی سازمان (Australasia Archives council, 2006, page 18-23)

استانداردهای مدیریتی ارائه شده در خصوص امنیت اطلاعات و ارتباطات

سازمان‌ها، عبارتند از:

- استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس
- استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد
- گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد()

کنترل‌های امنیتی در سیستم‌های اطلاعاتی

مجموعه کنترل‌های امنیتی موردنیاز سیستم‌های اطلاعاتی و ارتباطی هر سازمان، در قالب ده دسته‌بندی کلی شامل موارد زیر، ارائه شده است:

۱- تدوین سیاست امنیتی سازمان

ضرورت تدوین و انتشار سیاست‌های امنیت اطلاعات و ارتباطات سازمان، بنحوی که کلیه مخاطبین سیاست‌ها در جریان جزئیات آن قرار گیرند در این مرحله تامین میگردد. همچنین جزئیات و نحوه نگارش سیاست‌های امنیت اطلاعات و ارتباطات میان سازمانی ارائه میگردد.

۲- ایجاد تشکیلات تامین امنیت سازمان

تشریح ضرورت ایجاد تشکیلات امنیت اطلاعات و ارتباطات سازمان، جزئیات این تشکیلات در سطوح سیاستگذاری، اجرائی و فنی به همراه مسئولیت‌های هر یک از سطوح در این مرحله صورت میگیرد.

۳- دسته‌بندی سرمایه‌ها و تعیین کنترل‌های لازم

در این قسمت، ضمن تشریح ضرورت دسته‌بندی اطلاعات سازمان، به جزئیات تدوین راهنمای دسته‌بندی اطلاعات سازمان پرداخته و محورهای دسته‌بندی اطلاعات را ارائه نموده است.

۴- امنیت پرسنلی

در این قسمت، ضمن اشاره به ضرورت رعایت ملاحظات امنیتی در بکارگیری پرسنل، ضرورت آموزش پرسنل در زمینه امنیت اطلاعات و ارتباطات، مطرح شده و لیستی از مسئولیت‌های پرسنل در پروسه تامین امنیت اطلاعات و ارتباطات سازمان، ارائه شده است.

۵- امنیت فیزیکی و پیرامونی

در این قسمت، اهمیت و ابعاد امنیت فیزیکی، جزئیات محافظت از تجهیزات و کنترل‌های موردنیاز برای این منظور، ارائه شده است.

۶- مدیریت ارتباطات

در این قسمت، ضرورت و جزئیات روالهای اجرائی موردنیاز، بمنظور تعیین مسئولیت هر یک از پرسنل، روالهای مربوط به سفارش، خرید، تست و آموزش سیستم‌ها، محافظت در مقابل نرم‌افزارهای مخرب، اقدامات موردنیاز در خصوص ثبت وقایع و پشتیبان‌گیری از اطلاعات، مدیریت شبکه، محافظت از رسانه‌ها و روالها و مسئولیت‌های مربوط به درخواست، تحویل، تست و سایر موارد تغییر نرم‌افزارها ارائه شده است.

۷- کنترل دسترسی

برای حراست از اطلاعات، باید دسترسی به اطلاعات کنترل شود. افراد مجاز باید توانایی دسترسی به اطلاعات موردنیاز جهت ارائه خدمات بهتر را داشته باشند. دسترسی به اطلاعات حفاظت شده باید محدود باشد به افراد، برنامه‌های کامپیوتری، فرآیندها و سیستم‌هایی که مجاز به دسترسی به اطلاعات هستند. این امر مستلزم وجود مکانیزم‌های برای کنترل دسترسی به اطلاعات حفاظت شده می باشد. پیچیدگی مکانیزم‌های کنترل دسترسی باید مطابق با ارزش اطلاعات مورد حفاظت باشد. اطلاعات حساس تر و با ارزش تر نیاز به مکانیزم کنترل دسترسی قوی تری دارند. اساس مکانیزم‌های کنترل دسترسی بر دو مقوله احراز هویت و تصدیق هویت است.

احراز هویت تشخیص هویت فردی است که درخواست دسترسی به اطلاعات را دارد. قبل از اینکه به کاربری اجازه دسترسی به اطلاعات حفاظت شده داده شود ضروری است که هویت این فرد بررسی شود که او چه کسی است. تصدیق هویت عمل تایید هویت است. زمانی که صحت اطلاعات خواسته شده از کاربر تایید شود، تصدیق هویت انجام می‌شود.

از سه نوع اطلاعات می توان برای احراز و تصدیق هویت فردی استفاده کرد. مواردی از قبیل کد، رمز عبور، کارت مغناطیسی ابزارهایی هستند که در احراز و تصدیق استفاده می شوند. اخیراً تکنیک‌های بیومتریک مانند اثر انگشت، اثر کف دست، صدا و اسکن شبکه چشم نیز استفاده می شوند. ترکیبی از این اطلاعات می تواند احراز و تصدیق هویت قوی را میسر گرداند. در سیستم‌های کامپیوتری امروزی، نام کاربری رایج‌ترین شکل احراز و رمز عبور رایج‌ترین شکل تصدیق هویت است.

پس از آنکه فرد یا کاربر با موفقیت احراز و تصدیق هویت شد باید تعیین کرد که او مجاز به دسترسی به چه منابع اطلاعاتی و انجام چه اقداماتی روی آنها است مثل نمایش اسناد، ایجاد یک سند جدید، حذف اطلاعات گذشته و یا تغییر اطلاعات موجود. این عمل با صدور مجوز و تعریف سطوح مختلف دسترسی انجام می گیرد.

صدور مجوز برای دسترسی به اطلاعات و خدمات کامپیوتری با برقراری سیاست و روش‌های مدیریتی آغاز می شود. رویکردهای کنترل دسترسی مختلفی وجود دارند. سه رویکرد شناخته شده وجود دارند که عبارتند از: رویکرد صلاح دیدی، غیرصلاح دیدی و اجباری.

در رویکرد صلاح دیدی سیستم منابع اطلاعات قابلیت دسترسی به منابع خود را تعیین می کند. رویکرد غیر صلاح دیدی تمام کنترل دسترسی متمرکز است و به صلاح دید کاربر نیست. در روش اجباری، دسترسی به اطلاعات و یا محروم کردن بسته به طبقه بندی اطلاعات و رتبه فرد خواهان دسترسی دارد.

۸- نگهداری و توسعه سیستم‌ها

در این قسمت، ضرورت تعیین نیازمندی‌های امنیتی سیستم‌ها، امنیت در سیستم‌های کاربردی، کنترل‌های رمزنگاری، محافظت از فایل‌های سیستم و ملاحظات امنیتی موردنیاز در توسعه و پشتیبانی سیستم‌ها، ارائه شده است.

۹- مدیریت تداوم فعالیت سازمان

در این قسمت، رویه‌های مدیریت تداوم فعالیت، نقش تحلیل ضربه در تداوم فعالیت، طراحی و تدوین طرح‌های تداوم فعالیت، قالب پیشنهادی برای طرح تداوم فعالیت سازمان و طرح‌های تست، پشتیبانی و ارزیابی مجدد تداوم فعالیت سازمان، ارائه شده است.

۱۰- پاسخگویی به نیازهای امنیتی

در این قسمت، مقررات موردنیاز در خصوص پاسخگوئی به نیازهای امنیتی، سیاست‌های امنیتی موردنیاز و ابزارها و مکانیزم‌های بازرسی امنیتی سیستم‌ها، ارائه شده است.

نتیجه گیری

در اغلب موارد، تشکیلات سازمانی همچون شبکه های کامپیوتری در برابر تغییرات فشرده و ناگهانی با ضعف و شکست مواجه می شوند. یک پروژه امنیتی نیز از این مقوله مستثنا نیست. قبل از پیاده سازی هر چیزی، ابتدا باید طرح و برنامه آن را تعیین و سپس ابزار لازم را مهیا کرد. امنیت بالاتر شبکه در سازمان تنها به داشتن یک دیوار آتش ختم نمی شود بلکه برای دستیابی به این مقوله بسیار مهم باید به طور دقیق مشخص شود که چه اطلاعاتی باید مورد مدیریت و تامین امنیت قرار بگیرند. سطح دسترسی هر کاربر چقدر باشد تا ضمن انجام مسئولیت های محوله از اقدامات خرابکارانه وی مثل نسخه برداری، تغییر و دستکاری جلوگیری به عمل آید. ضمناً به طور جزئی تر باید مشخص شود برای پیاده سازی امنیت در سازمان چه سیاستی را در پیش گرفت تا مدیریت و امنیتی را که در نظر دارد پیاده سازی نماید.

REFERENCES

1. Helena Halas et.al, "Towards secure legally valid long-term electronic archive using pattern approach", 2008.
2. An open text on "A Special Guide on Document Management".
3. Brendan E. Asogwa et.al, "The Challenges of Preservation of Archives and Records in the Electronic Age", 2012.
4. National Archives of Australia, "Digital archiving in the 21st century, 2006.

نقش آفرینی ثبت احوال نوین در توسعه و پیاده سازی دولت

الکترونیک

مهدی سعادت پور^۱

چکیده

در عصر حاضر شاهد تغییر و تحولات مداوم در شرایط و روش های انجام کسب و کار هستیم و هر روز نوآوری های جدیدی را در این خصوص تجربه می نماییم . در سال های اخیر به واسطه رشد سریع فناوری اطلاعات و ارتباطات و از همه مهمتر گسترش اینترنت ، روند این تغییرات تسریع یافته است . گرایش به سمت الکترونیکی کردن کارها در حوزه خدمات دولتی به خوبی مشهود می باشد . به طوری که حاصل این گرایش در قالب سیستم دولت الکترونیک تجلی یافته است.

خدمات در دولت الکترونیک بر اساس ارتباط بین جامعه مشتریان با جامعه سامانه های کاربردی الکترونیکی شکل می گیرد. روابط گوناگون میان شهروندان حقیقی و بنگاه های حقوقی با دولت ، زمینه ساز ارائه انواع خدمات در بستر دولت الکترونیکی خواهد بود که باعث ایجاد مفهومی تحت عنوان "جامعه سامانه های الکترونیکی دولت" می شود. آنچه که به عنوان کلید اصلی ورود متقاضیان و مشتریان خدمات در دولت الکترونیک به جامعه سامانه های الکترونیکی دولت می شود ، مفهوم هویت الکترونیکی می باشد. در واقع سازمان ثبت احوال با ارائه « شماره ملی » در قالب کارت شناسایی ملی به عنوان کلید منحصر به فرد برای دسترسی به هویت افراد حقیقی یکی از مهمترین گام ها را برای تحقق دولت الکترونیک در برداشته است. سیستم ثبت احوال یک سیستم مادر است که نقش حیاتی در اداره و کنترل امور جامعه و برنامه ریزی های کلان کشور دارد. همسویی با تکنولوژی روز دنیا برای ارائه خدمات الکترونیکی ، نشانه پویایی و کارآمدی سازمان ثبت احوال است و انجام طرح های بزرگی همچون کارت هوشمند ملی، صدور شناسنامه های الکترونیکی، آرشیو الکترونیکی اسناد سجلی

^۱ - اداره ثبت احوال کازرون ایمیل : mahdi61saadat@gmail.com

و ایجاد پایگاه اطلاعات جمعیتی از نقش مهم ثبت احوال در استقرار دولت الکترونیک و روزگاری نوین این سازمان حکایت دارد.

اکنون جایگاه نظام نوین ثبت احوال در قلب خدمات مشاع زیرساخت دولت الکترونیکی کشور بسیار کلیدی و پر اهمیت است و تحقق آن یکی از شروط لازم شفافیت سایر ابعاد هویتی شهروندان و تحقق سامانه های کاربردی الکترونیکی در بستر دولت الکترونیک می باشد. البته در مسیر پیاد سازی و توسعه دولت الکترونیک سازمان ها با مشکلاتی نظیر عوامل فرهنگی، عوامل سازمانی اداری و کمبود منابع روبرو هستند که می توان با اقدامات مناسب و به موقع نظیر آموزش و ... این موانع را کم اثر و حتی بی تاثیر ساخت.

واژه های کلیدی: دولت الکترونیک، شهروند، سازمان ثبت احوال

کلید واژه ها

دولت الکترونیک: دولت الکترونیک استفاده از فناوری های اطلاعاتی و ارتباطی به منظور ارائه خدمات دولتی، به صورت بهنگام و مستقیم به شهروندان، در ۲۴ ساعته شبانه روز و ۷ روز هفته است. دولت الکترونیک به افراد تسهیلات لازم جهت دسترسی مناسب به اطلاعات و خدمات دولتی و فرصت های گسترده تر برای مشارکت در فرایندها را ارائه می نماید.

شهروند: فردی با حقوق و مسئولیت های تعریف شده و معین در جامعه؛ این حقوق شامل حق رأی، حق اظهار نظر آزاد و ... می شود. افرادی که در انتخابات شرکت کرده و رأی می دهند و یا اشخاصی که در یک تجمع سیاسی سخنرانی می کنند، مشتریان دولت نیستند؛ بلکه شهروندانی هستند که در فعالیت های جامعه شرکت می کنند.

مشتری: استفاده کننده از سرویس های دولتی را مشتری می گویند، مانند بازنشستگانی که حقوق بازنشستگی دریافت می کنند و یا افرادی که برای معالجه به کلینیک های دولتی مراجعه می نمایند.

سازمان ثبت احوال کشور: یکی از سازمانهای دولتی ایران واز نهاد های زیر مجموعه وزارت کشور است که جمع آوری اطلاعات و آمار جمعیتی کشور ایران را به عهده دارد. این سازمان وظیفه تهیه اطلاعات ثبتی اساسی مانند زاد و ولد، مرگ و میر، ازدواج و طلاق و نیز صدور مدارک هویتی مانند شناسنامه و کارت شناسایی ملی را بر عهده دارد.

داده های ثبتی: داده های ثبتی، داده هایی هستند که در حین انجام فعالیت های عینی، واقعی و جاری یک سازمان و با استفاده از فرمها، اسناد، مدارک و فایل های کامپیوتری موجود در داخل سازمان ثبت می شوند.

نظام آمارهای ثبتی: نظام آمارهای ثبتی، نظامی است که داده های مناسبی در درون خود ثبت کرده و این داده های ثبتی را به آمارهای ثبتی موردنیاز کاربران تبدیل کرده و آنها را به نحو مناسب در اختیار آنان قرار می دهد.

مقدمه:

در سال های اخیر به واسطه رشد سریع فناوری اطلاعات و ارتباطات و از همه مهمتر گسترش اینترنت، روند این تغییرات تسریع یافته است. گرایش به سمت الکترونیکی کردن کارها در حوزه خدمات دولتی به خوبی مشهود می باشد. به طوری که حاصل این گرایش در قالب سیستم دولت الکترونیک تجلی یافته است.

بنابر این در دوران کنونی یعنی عصر اطلاعات و جایی که دولت ها به سوی الکترونیکی شدن در حرکت هستند مدیران و مسئولان در تمامی سطوح و همچنین شهروندان نیازمند درکی صحیح از فناوری اطلاعات هستند این ها افرادی هستند که فرایند اصلاح را پیش خواهند برد، پس باید از مشکلات و فرصت های پیش رو شناختی شفاف داشته باشند. در این راستا پروژه های توسعه دولت الکترونیک باید به گونه ای طراحی و انجام شوند که به افزایش مشارکت شهروندان در فرایندهای دولتی، تسهیل بوروکراسی اداری و صرفه جویی در زمان و منابع موجب شود. روشن است که مفهوم دولت الکترونیک حول محور شهروند معنی پیدا می کند. بر این اساس به موضوع دولت الکترونیک صرفا نباید از منظر کاهش هزینه یا افزایش کارایی پرداخت. بلکه باید بهبود زندگی شهروندان عادی را به عنوان یکی از اهداف اصلی دولت الکترونیک در نظر گرفت. فقط در این صورت است که دولت الکترونیک از حمایت مردمی برخوردار می شود. در این میان مشورت با شهروندان درباره طراحی سیستم ها و برنامه های کاربردی که حول محور شهروندان می گردد اهمیت فراوان دارد در عین حال که برنامه ریزان و قانون گذاران باید تفاوت های بومی و فرهنگی مناطق مختلف را در نظر بگیرند. با ظهور فناوری های اطلاعاتی و ارتباطی و نفوذ آن بر ابعاد زمانی و مکانی جامعه، اهمیت نقش سازمان ها و ادارات در پیاده سازی و توسعه دولت الکترونیک در کشور مشخص می شود. بنابراین می توان

به اهمیت نقش آمار در توسعه پایدار و همچنین در اختیار داشتن اطلاعات صحیح و به روز که یکی از پیش نیازها در تمام تصمیم گیری ها و سیاست گذاری ها و برنامه ریزی های کشور است، پی برد. در این راستا سازمان ثبت احوال با قرار داشتن در قلب بخش خدمات مشاع زیرساخت دولت الکترونیکی کشور و نیز با بهره گیری از آخرین فناوری های روز دنیا و مکانیزاسیون فرایندهای اصلی سازمانی خود اقدامات موثری را در جهت ارائه بهتر خدمات الکترونیکی به شهروندان، سایر سازمان های دولتی و پرسنل خود سازمان ثبت احوال و در نتیجه آن، توسعه و پیاده سازی دولت الکترونیک در کشور به انجام رسانیده است که در ادامه به بررسی این نقش آفرینی می پردازیم. امید است که بتوان با یک برنامه ریزی جامع و استفاده از همه ظرفیتهای موجود در سازمان ها و نهادهای کشور به توسعه ای پایدار در دولت الکترونیک دست یابیم.

دولت الکترونیک

استفاده دولت ها از فناوری اطلاعاتی و ارتباطی جدید جهت ارائه خدمات به شهروندان، زمینه ساز استقرار یک سیستم دولتی نوین در دنیا گردیده است که هم از لحاظ ساختاری و هم از لحاظ کارکرد با سیستم های دولتی گذشته متفاوت است، در این سیستم دولت بجای اینکه حاکم بر مردم باشد خدمتگزار مردم خواهد بود. خدمات و اطلاعات در کوتاه ترین زمان و با برترین کیفیت به شهروندان ارائه می شود و زمینه مشارکت هر چه بیشتر شهروندان در اداره امور عمومی فراهم می گردد. این سیستم دولتی نوین همان دولت الکترونیک است.

دولت الکترونیک بیانگر گرایش دولت ها به استفاده از سیستم ها و فناوری های اطلاعاتی به منظور افزایش دسترسی شهروندان به اطلاعات و خدمات و دولتی می باشد. سازمان های دولتی با استفاده از شبکه های ارتباطی، شرایطی را برای برقراری ارتباطات راحت تر و سریع تر مردم با خود فراهم می آورند. هدف از به کارگیری دولت الکترونیک در اداره ی کشورها، تسهیل امور دولت و آرایه ی سریع تر و با کیفیت تر خدمات دولتی به شهروندان یک کشور است. از مهم ترین کاربردهای IT در امور کشورداری است. در دولت الکترونیک بسیاری از فرآیندهای امور اداری دولت به صورت الکترونیک و از طریق استفاده ی فراگیر از تکنولوژی اطلاعات صورت می پذیرد، مانند صدور گواهینامه ی رانندگی، پرداخت مالیات ها، ثبت اسناد، پرداخت بیمه ی بازنشستگی و درمان، کنترل ترافیک، صدور پاسپورت، ویزا و ... است که با نگاهی ساده به

موضوع متوجه نقش کلیدی سازمان ثبت احوال در ارائه اطلاعات و آمار مورد نیاز سازمان ها و در نتیجه اجرای روان تر دولت الکترونیک خواهیم شد. بنابراین، دولت حجم عظیمی از اطلاعات را جمع‌آوری می‌کند که اغلب دسترسی سازمان ها و افراد به این اطلاعات مشکل است. دولت الکترونیک می‌تواند دسترسی به اطلاعات را فراهم سازد و مدیریت امور اداری کشور با استفاده از فناوری اطلاعات ثمربخش‌تر، باکیفیت بالاتر و کارآتر، با سرعت بیشتر و هزینه کمتر انجام گیرد.

ثبت احوال از گذشته تا امروز

"سازمان ثبت احوال کشور" سازمانی با شخصیت حقوقی مستقل از لحاظ اداری، مالی، و اجرایی و از حیث تشکیلاتی در دولت وابسته به وزارت کشور است. این سازمان بصورت متمرکز اداره می‌شود و کلیه ادارات در سطح کشور تابع ستاد مرکزی بوده و آئین نامه ها و دستور العمل های مصوب ابلاغی را اجرا می‌نماید. به دلیل گستردگی وظایف قانونی، "سازمان ثبت احوال کشور" در اقصی نقاط کشور به ارائه خدمات مشغول بوده و پر مراجعه ترین سازمان دولتی است.

ثبت احوال بصورت یکپارچه و منسجم در جهان مربوط به قرن نوزدهم میلادی است. در ایران همزمان با نوسازی و مدرنیزاسیون و نیاز به شناسایی اتباع جهت ایجاد ارتش منظم، اخذ مالیات و... تاسیس ثبت احوال در دستور کار قرار گرفت از این رو در جلسه مورخه ۳۰ آذر ماه ۱۲۹۷ هجری شمسی به تصویب هیات وزیران رسید و با صدور اولین شناسنامه برای دختری به نام فاطمه ایرانی در تاریخ ۳ دیماه ۱۲۹۷ در تهران فعالیت خود را آغاز کرد.

تا قبل از سال ۱۲۹۵ هجری شمسی ثبت وقایع حیاتی از جمله ولادت و وفات براساس اعتقادات مذهبی و سنت های رایج در کشور، با نگارش نام و تاریخ ولادت مولود در پشت جلد کتب مقدس از جمله قرآن مجید به عمل می‌آمد و از افراد متوفی نیز جزء نام و تاریخ وفات آنان که بر روی سنگ قبر ایشان نگاشته می‌شد اثری مشاهده نمی‌گردید. با گسترش فرهنگ و دانش بشری و نیز توسعه روز افزون شهرها و روستاها و افزایش جمعیت کشور، نیاز به سازمان تشکیلاتی برای ثبت وقایع حیاتی ضرورتی اجتناب ناپذیر می‌نمود. به تدریج فکر تشکیل سازمان متولی ثبت ولادت و وفات و نیز صدور شناسنامه برای اتباع کشور قوت گرفت.

از آن زمان تاکنون به تناسب شرایط زمانی تغییر و تحولات بوجود آمده در کشور و با احساس عدم تناسب قوانین موجود با نیازهای جامعه، قانون ثبت احوال نیز به دفعات مورد

تجدید نظر، تغییر و اصلاح قرار گرفت. پس از گذشت این زمان در تیر ماه ۱۳۵۵ قانون جدید ثبت احوال مشتمل بر ۵۵ ماده به تصویب رسید و سپس به موجب اصلاحیه دی ماه سال ۱۳۶۳ مجلس شورای اسلامی در برخی از مواد اصلاحاتی صورت گرفت و تاکنون نیز این قانون به قوت خود باقی مانده است. سرانجام با تصویب قانون تقسیمات کشوری ادارات استانی و شهرستانی این سازمان نیز گسترش یافت و عنوان آن نیز به سازمان ثبت احوال کشور تغییر یافت. سازمان ثبت احوال کشور به دلیل در اختیار داشتن اسناد هویت و تابعیت فردی و آمارهای حیاتی یکی از ارکان مهم حکومت تلقی می شود. ارائه خدمات عمومی به آحاد مردم و اطلاعات ویژه جمعیتی به ارکان حکومت از ویژگی های اختصاصی و انحصاری این سازمان است.

در حال حاضر با ظهور فناوری های اطلاعاتی و ورود آن به سازمان ها باعث شده است تا سیستم های اطلاعاتی سازمان و فناوری های مورد استفاده آنها، از نقش تعیین کننده ای در انجام وظایف سازمانی برخوردار شوند. سازمان ثبت احوال کشور برای انجام مأموریت های محوله، و خدمات رسانی در زمینه امور سجلی و انفورماتیک با ایجاد ثبت احوال نوین با سه وظیفه ثبت وقایع حیاتی، صدور اسناد هویتی و انتشار داده های جمعیتی گام های مهمی در خصوص همراهی با تغییرات سریع و مداوم عصر فناوری اطلاعات و در نتیجه تحقق دولت الکترونیک برداشته است. از جمله کارهای مهم ثبت احوال، ایجاد ثبت احوال نوین با سه وظیفه مذکور با تاکید بر نقش مهم سازمان در دولت الکترونیک است و این با هدف استقرار نظام جامع شناسائی ایرانیان و استقرار سازمان الکترونیک و ترسیم راهبردها و تحقق آن به شکل نوین برنامه ریزی شده است، که از جمله این اقدامات طراحی و صدور کارت هوشمند ملی ایرانیان است. همچنین از جمله راهبردهای اساسی سازمان ایجاد آرشیو الکترونیکی و خدمت رسانی به صورت مکانیزه است، به طریقی که هر اداره برای خود دارای سایت مجزا باشد. بنابراین همزمان با تحولات صورت گرفته در حوزه فناوری اطلاعات و ارتباطات و لزوم ایجاد و ارائه خدمات بر بستر الکترونیک جهت ارائه خدمات سریع، صحیح و کم هزینه، سازمان ثبت احوال نیز اقدامات اساسی را در جهت ارائه خدمات درون سازمانی و برون سازمانی آغاز نموده است.

پس در سخنی کوتاه می توان گفت اکنون سازمان ثبت احوال یکی ابرزارهای کلیدی کشور در امور حاکمیتی و برنامه ریزی های کلان به شمار می رود. همسویی با تکنولوژی روز دنیا برای ارائه خدمات الکترونیکی، نشانه پویایی و کارآمدی سازمان ثبت احوال است و انجام

طرح های بزرگی همچون کارت هوشمند ملی ، صدور شناسنامه های الکترونیکی ، آرشیو الکترونیکی اسناد سجلی و ایجاد پایگاه اطلاعات جمعیتی از نقش مهم ثبت احوال در استقرار دولت الکترونیک و روزگاری نوین این سازمان حکایت دارد.

ثبت احوال، دریچه دولت الکترونیک

دولت الکترونیک به معنای فراهم کردن شرایطی است که دولت ها بتوانند خدمات خود را به صورت شبانه روزی و در تمام ایام هفته به شهروندان ارائه کنند. این امر در سال های اخیر به طور جدی در دستور کار دولت ها قرار گرفته است و دولت مردان هوشمند نیروهای خود را در راه تحقق چنین شرایطی بسیج کرده اند و در صدد برآمدند که فرایندهای موجود در جامعه را با کمک فناوری نوین ارتباطات و اطلاعات اصلاح کرده و از این طریق به شیوه کارآمدتری به ارائه خدمات به شهروندان بپردازند. یکی از مهم ترین نتایج مورد انتظار از دولت الکترونیک افزایش رضایتمندی مردم از طریق افزایش سرعت ، دقت و صرفه جویی در هزینه ها است. به دلیل ماهیت وظایفی که بر عهده سازمان ثبت احوال است از جمله ثبت وقایع حیاتی چهارگانه، این سازمان از اطلاعات انسانی غنی برخوردار است که توجه و جهت دهی به آن می تواند به عنوان موتور محرکه توسعه نظام اداری و مبنای زیرساخت دولت الکترونیک قرار گیرد.

سیستم ثبت احوال یک سیستم مادر است که نقش حیاتی در اداره و کنترل امور جامعه دارد. سیستم ثبت احوال با استفاده از داده های ثبتی مهم ترین آمارهای ثبتی جمعیت کشور را نیز تولید می کند و در مواردی می تواند مبنای محاسبه بعضی از شاخص های اجتماعی مورد نیاز برنامه ریزی قرار گیرد. طی سالهای اخیر با تخصیص شماره شناسایی و استقرار پایگاه اطلاعات جمعیت، خدمات سازمان ثبت احوال کشور بهبود قابل ملاحظه ای یافته است. علاوه بر این، سازمان ثبت احوال با ارائه اطلاعات هویتی به سازمان های مجاز ، متناسب با درخواست و گزارشات مختلف در زمینه آمار انسانی به صورت دوره ای یا بر حسب درخواست در عرضه اطلاعات هویتی و آمار انسانی قدم های مؤثری برداشته است. با توجه به تعاملات اجتماعی و اهمیت فرایند تشخیص هویت برای انجام امور مختلف مردم و نیز رشد روز افزون فناوری اطلاعات و ارتباطات، سازمان ثبت احوال با ارائه خدمات مختلف در حوزه احراز هویت توانسته است جهت سهولت خدمات رسانی به مردم از سوی دولت اثر چشم گیری بگذارد و در نتیجه راندمان و کارایی ارکان دولت در تعامل با مردم به طور چشم گیری افزایش یافته است. یکی از

مهم ترین اولویت هایی که سازمان ثبت احوال کشور در دنبال و اجرا می کند استفاده از شیوه الکترونیکی در زمینه ثبت و نگهداری اسناد است. بر این اساس طرح های مختلفی از سوی این سازمان در سال های اخیر در حال انجام است تا روند فعالیت ثبت احوال از حالت سنتی گذشته خود خارج شود. که می توان به طرح هایی از قبیل صدور شناسنامه های مکانیزه، آرشیو الکترونیکی اسناد و صدور کارت ملی هوشمند اشاره کرد که از اقدامات ثبت احوال در راستای الکترونیکی کردن فعالیت های خود است. در واقع در پیچه دولت الکترونیک، ثبت احوال است و این سازمان با گسترده خدماتی که ارائه می کند به سمت دولت الکترونیک قدم های بسیار مثبت و رو به جلویی برداشته است.

جایگاه ثبت احوال در پیاده سازی انواع دولت الکترونیک

در واقع ستون اصلی دولت الکترونیک، ارتباطی است که دولت با شهروندان، بنگاه های اقتصادی، کارکنان و سایر مؤسسات دولتی برقرار می سازد و این ارتباطات است که روح دولت الکترونیک را تشکیل می دهد (اکوت اوما و کافری، ۲۰۰۰). به عبارت دیگر دولت الکترونیکی ترکیبی از فناوری اطلاعات و شبکه اطلاع رسانی وب است که هدف آن ارائه مستقیم خدمات به شهروندان، بخش های تجاری و کارکنان و سایر بخش های دولتی است. در این قسمت سعی می کنیم ابعاد مختلف دولت الکترونیک و روابط بین آنها را بشناسیم و جایگاه ثبت احوال در پیاده سازی این ابعاد را بیان کنیم. دولت الکترونیک برای سرویس دهی به شهروندان، واحدهای خصوصی و سازمان های دولتی دیگر، از مجراهای مختلفی استفاده می کند که این خود به روابطی مابین دولت و ارکان جامعه می انجامد که تحت عناوین زیر دسته بندی می شوند:

تعاملات دولت با شهروندان

رابطه دولت با شهروندان که طی آن دولت خدمتی را به شهروندان ارائه می دهد. در اینجا شهروند به عنوان عضوی از جامعه که حق او استفاده از خدمات دولت الکترونیک است، این خدمات را به صورت رایگان دریافت می کند. این نوع از طبقه بندی از ارائه خدمات بر توانا ساختن دولت و شهروندان جهت تبادل اطلاعات با یکدیگر به شیوه کارآمد و الکترونیکی تمرکز دارد. در واقع برای ارائه خدمات و اطلاعات به افراد جامعه استفاده می شود.

این مؤلفه مهمترین و گسترده ترین نوع تعاملات است و دامنه متفاوتی از تسهیلات و خدمات را برای مردم فراهم می کند در این راستا ثبت احوال نوین با اجرای پروژه های مرتبط با

ارائه خدمات الکترونیک در بستر پورتال سازمان گام های موثری برداشته است. از راهبردهایی که سازمان ثبت احوال جهت خدمت رسانی به صورت مکانیزه در دست اجرا دارد، هر اداره برای خود دارای سایت مجزا می باشد و با مکانیزه کردن سیستمهای ارائه خدمات خود به شهروندان توانسته است امکان ارائه خدمات نوین الکترونیکی یکسان به مردم در شهر و روستا داشته باشد. همچنین با توجه به اینکه یکی از تفاوت های ثبت احوال با دیگر دستگاه های دولتی، حاکمیتی بودن و خدمات دو سویه به مردم و دولت است بر این اساس بسیاری از خدمات را بایستی خود مستقیم به مردم ارائه نماید. برای این امر حضور در اقصی نقاط کشور از برنامه های ثبت احوال می باشد. که با راه اندازی نمایندگی در بخش ها و مراکز درمانی و آرامستان ها که نیاز به خدمات بیشتری (در زمینه ثبت وقایع حیاتی) است که این مهم بوسیله استقرار ونوسازی تجهیزات رایانه ای و ایجاد پهنای باند شبکه ارتباطی الکترونیکی با بهره گیری از فیبر نوری تحقق یافته است. از دیگر اقدامات سازمان ثبت احوال، اتصال تجهیزات ادارات به دستگاه pos (کارت خوان) متصل به شبکه شتاب و در نتیجه به وجود آمدن شرایطی راضی کننده برای ارباب رجوع و ارائه خدمات سریع به آنان می باشد.

تعاملات دولت با دولت

رابطه ای بین سازمان های درون دولت و یا بین دولت های مختلف که طی آن، هریک از این سازمان ها یا دولت ها می توانند به دیگری سرویس دهند و یا روابطی در زمینه های مختلف داشته باشند. اکثر امور اداری دولت به نحوی به هم مربوط هستند. بدین معنی که اطلاعات یک سازمان یا بخش مورد استفاده، از سرعت و اطمینان کافی برخوردار نیست. به همین دلیل نیاز به اتصال سازمان های مختلف دولتی احساس می شود.

این نوع تعاملات به دلیل محرمانه بودن آن بیشتر بر روی شبکه های خصوصی با ضریب امنیت بالا انجام می گیرد. در واقع این نوع دولت جهت بهبود کارایی تبادل اطلاعات بین تشکیلات دولتی با یکدیگر تلاش می کند. این روش به دولت امکان می دهد که به وسیله حذف دوباره کاری ها ارتباطات را بهبود بخشد. سازمان ثبت احوال کشور با اجرای پروژه های مرتبط با تحقق سازمان الکترونیکی در تعاملات ستادی با سایر ادارات سراسر کشور اقدامات مهمی نظیر تحقق امکان بهره برداری آماری از پایگاه اطلاعات جمعیت کشور به صورت لحظه ای برای ادارات سراسر کشور در قالب پیاده سازی سامانه بر خط گزارشات آماری، ارتباط مرکز داده

سازمان با کلیه بانک های اطلاعاتی دستگاه های دولتی و دفاتر پیشخوان دولت به منظور استعلام بر خط هویت متقاضیان در تمامی مبادی ذیربط و یا مشارکت موثر در برگزاری انتخابات مکانیزه برداشته است. همچنین با توجه به اینکه در شرایط کنونی دیگر پذیرفته نیست که ارتباطات بین ادارات بصورت سنتی برقرار شود سازمان ثبت احوال با راه اندازی سیستم اتوماسیون اداری اقدامی مفید در تحقق دولت الکترونیک برداشته است. استفاده از سیستم های حوزه «اتوماسیون اداری»، کلیه نیازهای مربوط به ارتباطات، تبادل اطلاعات و مدیریت زمان و کارها را در سازمان برآورده می نماید و بستری بسیار قوی و مناسب جهت مکانیزاسیون در ابعاد مختلف مهیا می کند.

تعاملات دولت با کارمند

رابطه بین دولت با کارمندانش است و شامل خدماتی است که از طرف دولت به کارمندان اداری سازمان های دولتی در رابطه با کار و شغل آنها ارائه می شود. در این نوع از تعامل، شیوه های انجام هرچه بهتر ارائه خدمات به کارمندان دولتی آموزش داده می شود و کارمندان با استفاده از اینترنت و دیگر شبکه های خصوصی می توانند به اطلاعات جدید شغلی، تسهیلات اعطائی و... دسترسی پیدا نمایند. به این نوع دولت الکترونیک دولت با « اثربخشی و کارایی درونی » نیز گفته می شود. (ایوانز و یین، ۲۰۰۶: ۳) این سرویس ها می توانند شامل امور مالی، حقوقی و مالیات و ... مربوط به کارمندان باشد. همچنین رسیدگی به نحوه عملکرد کارمندان و ارتباطات داخلی یک سازمان دولتی جهت کاهش کاغذبازی و جلوگیری از اتلاف زمان و افزایش کارایی سازمان دولتی نیز می تواند از جمله کارکردهای این نوع ارتباط باشد. که سازمان ثبت احوال در موارد ذکر شده اقدامات مناسبی انجام داده است.

ثبت احوال و ویژگی های دولت الکترونیک

به طور کلی از رهگذر دولت الکترونیکی، اهدافی از قبیل کارایی و اثربخشی با کمک فن آوری اطلاعات به همراه خدمات آسان تر، ارزان تر و موثرتر برای دولت ها محقق می گردد. به بیان دیگر هدف دولت الکترونیک ارائه خدمات بهتر، با هزینه کمتر و اثر بخشی بیشتر است؛ ولی نمی توان استاندارد مشخصی برای سایر ویژگی های آن معرفی کرد، زیرا هر دولتی می تواند با توجه به نیازهای جامعه خودش نظام دولت الکترونیک را پایه ریزی کند. به طور کلی و در تعاریف عمومی، مشخصات یک دولت الکترونیک کارآمد را در قالب کلمه SMART (به معنی

هوشمند) بیان می کنند که هر یک از حروف این کلمه، نماینده یکی از ویژگی های دولت الکترونیک است که در ادامه، به بررسی عملکرد ثبت احوال در پیاده سازی این ویژگی ها و شاخص های کارآمدی دولت الکترونیک می پردازیم.

کوچک کردن (SMALL) S: دولت الکترونیک نباید گستردگی بیش از حد داشته باشد؛ تا بتواند از اتلاف نیروی انسانی و سرمایه جلوگیری کند. در این زمینه ثبت احوال از یک سو با در اختیار قرار دادن اطلاعات آماری و هویتی مورد نیاز سازمان ها و ارگان ها تشکیل دهنده دولت به صورت الکترونیکی از گستردگی و اتلاف سرمایه و نیروی انسانی جلوگیری و شرایط را جهت تصمیم گیری آسان تر سازمان ها بر اساس اطلاعات واصله و سرعت بخشیدن به اجرای امور فراهم می آورد و از سوی دیگر با حرکت سریع و حساب شده به سوی ثبت احوال نوین بوسیله الکترونیکی کردن فعالیت های درون سازمانی و همچنین خارج کردن فعالیتهای غیر محوری از محیط سازمان که به کوچک سازی می انجامد، نهایتاً منجر به افزایش کارایی و بهره وری اقتصادی دولت و همچنین صرفه جویی در وقت شهروندان و کاهش هزینه های آنها به وسیله خودکار شدن وظایف سازمان ها و افزایش سطوح و ارائه خدمات دولتی می گردد.

اخلاق (MORAL) M: دولت الکترونیک باید مقید به اخلاق بوده و حریم اطلاعات خصوصی شهروندان را حفظ نماید. ایمن سازی فضای مجازی در عرصه فناوری اطلاعات، دغدغه مهمی است که سازمان های ارائه دهنده خدمات به مردم باید به طور جدی به آن بپردازند. اولین گام و نخستین اقدام در این جهت ایجاد ساز و کار مدیریت هویت و شناسایی کاربران در فضای سایبری است. این گام مهم را سازمان ثبت احوال کشور برداشته است، سازمان ثبت احوال کشور با ایجاد پایگاه اطلاعات جمعیت کشور که یکی از بزرگترین بانک های اطلاعاتی در کشور است و آغاز پروژه بزرگ کارت هوشمند ملی، نقش مهمی در تشخیص و تصدیق هویت و به تبع آن صحت اعتبار و اصالت کاربران در فضای دیجیتالی ایفا خواهد کرد و به این ترتیب از سوءاستفاده های احتمالی توسط افراد سودجو در فضاهای مجازی جلوگیری می نماید. همچنین در این راستا سازمان ثبت احوال با توجه به در اختیار داشتن اطلاعات هویتی افراد که زیربنای و اساس هر فعالیت اداری و اقتصادی و فرهنگی می باشد وظیفه مهمی در حفظ و نگهداری این اطلاعات و جلوگیری از افشای آنها دارد که طبق دستورالعمل اجرایی ماده ۳۴ قانون ثبت احوال، «افشای اطلاعات مذکور در دفاتر ثبت کل وقایع و اسناد سجلی جز برای

صاحب سند و مقامات قضائی و دولتی ذیصلاح ممنوع است. « و سازمان ثبت احوال در این خصوص با توجه به الکترونیکی شدن فعالیت هایش و اهمیت امنیت اطلاعات در سامانه های ثبت احوال و به روز بودن اطلاعات ، اجرای کامل isms (امنیت شبکه) را در الویت برنامه ها یش قرار داده است.

رسیدگی کردن (AUDITABLE) A : دولت الکترونیک باید نسبت به فعالیت اجتماعی، اقتصادی و سیاسی که انجام می دهد جوابگو باشد؛ بدین معنی که بتوان تا حد امکان از روند پیشرفت این فعالیت ها آگاهی های لازم را کسب کند. ثبت احوال نوین در بکارگیری این ویژگی دولت الکترونیک با استقرار سیستم های الکترونیک فرصت بیشتری برای مشارکت افراد جامعه از تمامی بخش ها ، برای درگیری فعالتر در فعالیت های اجتماعی و اقتصادی و سیاسی فراهم می آورد و با استفاده از سیستم های گزارش گیری در زمینه انواع فعالیت های تحت پوشش خود از روند انجام امور آگاهی های لازم را کسب می نماید. **مسئول (RESPONSIBLE) R :** دولت الکترونیک باید در صورت بروز مشکلاتی ناشی از فعالیت هایش به مردم پاسخگو باشد. سازمان ثبت احوال در این خصوص در صورت مواجهه با تغییرات اطلاعات هویتی و یا مغایرت اطلاعات هویتی افراد در سامانه های دولتی چه در درون سازمان و چه در ارتباط با سایر سازمان های دولتی بلافاصله اقدام به اصلاح مغایرت و اعمال تغییرات می نماید که به صورت اتوماتیک در سامانه های الکترونیکی اجرا می گردد . همچنین سازمان ثبت احوال با راه اندازی سایت مجزا برای هر اداره و مکانیزه کردن سیستم های ارائه خدمات خود به شهروندان توانسته است امکان پاسخگویی الکترونیکی و همچنین ارائه خدمات نوین الکترونیکی یکسان به مردم در شهر و روستا داشته باشد.

شفاف (TRANSPARENT) T : دولت الکترونیک باید از موضع شفافیت در رابطه با امور شهروندان برخوردار باشد. ثبت احوال با فراهم کردن سیستم های مکانیزه برای ارائه خدمات به مردم چه در درون سازمان و چه در ارتباط با سایر سازمان ها موجب شفافیت و پاسخگویی در ارکان دولت را فراهم می آورد .

تاثیر سازمان ثبت احوال در توسعه و بکارگیری دولت الکترونیک

نقش سازمان ثبت احوال کشور در توسعه و پیاده سازی دولت الکترونیک از دو منظر قابل توجه است :

اول آنکه ، بستر سازی قانونی برای برقراری هرگونه خدمت ، مستلزم شناسایی است که در ارتباط با شناسایی ایرانیان این مهم به عهده سازمان ثبت احوال است. به همین جهت سازمان ثبت احوال کشور با طراحی و تولید حدود یک میلیارد شماره ملی امکان شناسایی هر فرد را با یک شماره ، در نظام های مختلف اداری فراهم نمود ، به طوری که هر فرد دارای یک شماره باشد و هر شماره نیز به یک فرد تخصیص داده شود . در واقع سازمان ثبت احوال با ارائه « شماره ملی » در قالب کارت شناسایی ملی به عنوان کلید منحصر به فرد برای دسترسی به هویت افراد حقیقی، یکی از مهمترین گام ها را برای تحقق دولت الکترونیک طی سال های گذشته برداشته است.

دوم آنکه این سازمان با در اختیار داشتن ادارات و نمایندگی ها در اقصی نقاط کشور و ارائه خدمات ، یکی از دستگاه های حاکمیتی است که بیشترین ارتباط با مردم و بسیاری دستگاه های اجرایی را دارد. بدین شکل که جزء محدود سازمان هایی است که موظف به ارائه خدمات به تمامی مردم (ایرانیان و در موارد خاصی از افراد غیرایرانی که اقامت قانونی در کشور دارند) و دستگاه های اجرایی دارد.

در این خصوص می توان به موارد ذیل اشاره نمود :

۱ : سازمان ثبت احوال با اجرای طرح سیستم ثبت وقایع حیاتی و ایجاد پایگاه مکانیزه اطلاعات جمعیت کشور و پایگاه مکانیزه عکس و نشانی ... از دستگاه های پیشستاز در مکانیزه نمودن ارائه خدمات بوده است . ایجاد و بهره برداری از پایگاه اطلاعات جمعیت کشور در سازمان ثبت احوال به منظور ثبت وقایع حیاتی در تمامی سطوح این سازمان از طریق شبکه اختصاصی تا سطح ادارات کل و ادارات ثبت احوال سراسر کشور این امکان را فراهم آورده که به محض ثبت یک واقعه در ادارات ثبت احوال، اطلاعات در پایگاه اطلاعات جمعیت کشور ذخیره گردیده و تهیه گزارش های آماری از اطلاعات موجود در هر دوره زمانی امکان پذیر باشد. اقدامات فوق باعث گردیده تا با ارتقای ابعاد کیفیت داده های ثبتی و استقرار کامل نظام آمارهای ثبتی در این سازمان، وضعیت تولید آمار و اطلاعات ثبتی جمعیتی در کشور به طور چشمگیری بهبود یافته و با تحقق این امر، زمینه های بسیار مناسبی برای محاسبه شاخص های جمعیتی، پایش تحولات جمعیتی، اتخاذسیاست های جمعیتی و تدوین برنامه های اجرایی متناسب فراهم گردد.

با ایجاد، راه اندازی و بهره برداری از پایگاه اطلاعات آماری کشور و سامانه برخط گزارشات آماری آن، تمامی اصول کلی و استانداردهای لازم الاجراء برای طراحی، ساخت و استقرار سیستم های اطلاعاتی- عملیاتی در حوزه های کاری نظام آمارهای ثبتی رعایت گردیده و نظام آمارهای ثبتی در این سازمان به طور کامل استقرار یافته است. طراحی نظام بر اساس یک متدولوژی از پیش معین شده و با طی دقیق همه مراحل مربوط صورت پذیرفته است. در هنگام طراحی نظام، سازماندهی لازم برای انتقال از وضع موجود به نظام جدید در هر یک از زیرسیستم ها در سراسر سازمان پیش بینی و رعایت شده است.

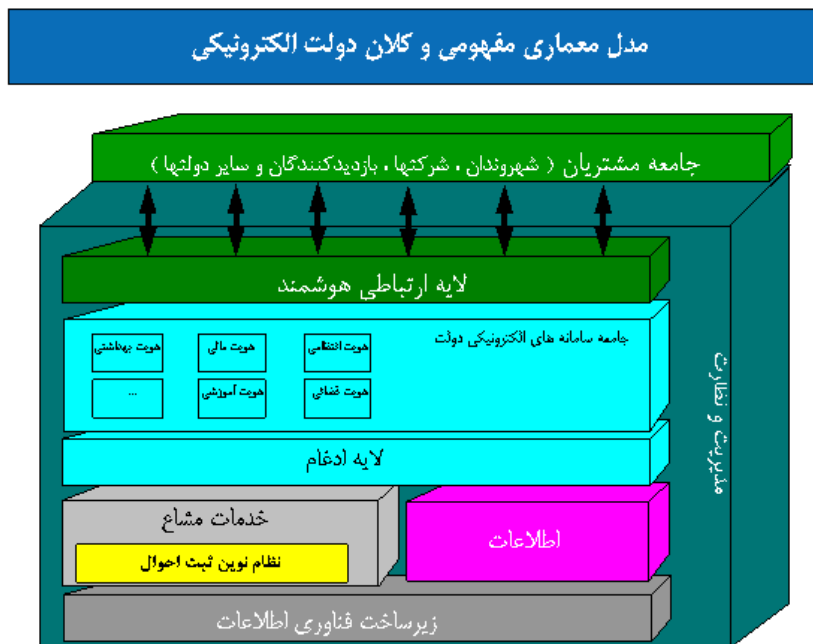
طراحی نظام به نحو جامعی صورت گرفته، بطوریکه پاسخگوی نیازهای آماری قابل تولید به روش ثبتی کاربران اعم از درون سازمانی و برون سازمانی می باشد. این نظام، سازمان را از جم عآوری آمار و اطلاعات بی نیاز ساخته است.

در طراحی نظام، سطح دسترسی کاربران مختلف به آمار و اطلاعات، تعیین و طبقه بندی شده و از اطلاعات خصوصی اشخاص حقیقی و حقوقی حفاظت می شود.

۲ : سند هویتی و شناسنامه «ام الاسناد» هر کشور است و بون شک مهمترین اقدام در جهت اتقان اسناد هویتی تلاش برای حفظ و صیانت از این اسناد است. سابقه قدمت اسناد هویتی که بعضا به یک قرن می رسد از یک سو و لزوم مراجعه متعدد به اسناد و اطلاعات مندرج در آن اسناد را همواره در معرض خطر فرسایش قرار می دهد. اهمیت حفظ و صیانت از این اسناد مهم در راستای اتقان اسناد هویتی، بیش از پیش لزوم ذخیره این اسناد در محیط های الکترونیک و مجازی را بیان می کند. از سوی دیگر به دلیل عدم امکان دسترسی به اطلاعات اسناد هر فرد در ادارات ثبت احوال غیر از محل صدور در بسیاری از مواقع افراد مجبور به مراجعه در ادارات ثبت احوال محل صدور خود جهت دریافت خدمات می شوند که این موضوع بعضا مشکلات زیادی را برای شهروندان ایجاد می نماید. این موارد باعث گردید سازمان ثبت احوال کشور طرح آرشيو الکترونیکی اسناد هویتی در دستور کار خود قرار دهد.

۳ : خدمات در دولت الکترونیک بر اساس ارتباط بین جامعه مشتریان با جامعه سامانه های کاربردی الکترونیکی شکل می گیرد. آنچه که به عنوان کلید اصلی ورود متقاضیان و مشتریان خدمات در دولت الکترونیک به جامعه سامانه های الکترونیکی دولت می شود، مفهوم هویت الکترونیکی می باشد. در واقع سازمان ثبت احوال با ارائه « شماره ملی » در قالب کارت

شناسایی ملی به عنوان کلید منحصر به فرد برای دسترسی به هویت افراد حقیقی یکی از مهمترین گام ها را برای تحقق دولت الکترونیک در سالیان گذشته برداشته است. هم اکنون گام مهم سازمان ثبت احوال در راستای تکمیل زیرساخت های لازم برای تحقق دولت الکترونیک که همان تعریف مفهوم شهروند الکترونیک می باشد، با اجرای پروژه کارت شناسایی ملی هوشمند در حال اجرا می باشد. که می توان مهمترین هدف از اجرای این پروژه را ایجاد امکان شناسایی و اثبات هویت و ارائه خدمات گوناگون به شهروندان در فضای دولت الکترونیک عنوان کرد. سازمان ثبت احوال کشور به عنوان مرجع امور هویتی کشور در نظر دارد تا کارتهای ملی هوشمند را جایگزین کارت های ملی فعلی کند. علاوه بر کاربردهای قبلی کارت ملی، کارت های جدید به عنوان کلید ورود به دولت الکترونیک و حرکت به سمت جامعه اطلاعاتی، این فرصت را فراهم می کند تا افراد به شیوه ای امن وارد فضای دیجیتالی شوند. کارت ملی هوشمند به عنوان مقدمه ای برای ورود به جامعه اطلاعاتی، می تواند موجب توزیع عادلانه فرصت ها، کاهش بسیاری از هزینه های دولت، مردم و بنگاه ها شود. و این امکان را فراهم می آورد که خدمات به روشی ساده، سریع و با کیفیت بالاتر به مردم ارائه شود و موجبات بهبود سطح کیفی زندگی مردم و بالابردن سطح رضایت مردم از دولت شود. لازم به ذکر است که ضریب امنیتی کارت هوشمند ملی بسیار بالاست، هیچ فردی نمی تواند بدون اجازه صاحب کارت و بدون وارد کردن پین کدهای تعیین شده توسط او به اطلاعات سطح دوم این کارت ها دسترسی پیدا کند. سطح اول اطلاعات این کارت ها همان اطلاعات شناسنامه ای افراد است که با اجازه او قابل مشاهده خواهد بود. شکل زیر جایگاه نظام نوین ثبت احوال را در لایه های مختلف مدل مفهومی دولت الکترونیکی نمایش می دهد:



همانگونه که شکل بالا نشان می دهد ، جایگاه نظام نوین ثبت احوال در قلب بخش خدمات مشاع زیرساخت دولت الکترونیکی کشور، بسیار کلیدی و پر اهمیت است و تحقق آن یکی از شروط لازم شفافیت سایر ابعاد هویتی شهروندان و تحقق سامانه های کاربردی الکترونیکی در بستر دولت الکترونیک می باشد.

همان طور که قبلا اشاره شد خدمات در دولت الکترونیک بر اساس ارتباط بین جامعه مشتریان با جامعه سامانه های کاربردی الکترونیکی شکل می گیرد. همانطور که قبلا نیز اشاره شد، روابط گوناگون میان شهروندان حقیقی و بنگاه های حقوقی با دولت ، زمینه ساز ارائه انواع خدمات در بستر دولت الکترونیکی خواهد بود که باعث ایجاد مفهومی تحت عنوان "جامعه سامانه های الکترونیکی دولت" می شود. آنچه که به عنوان کلید اصلی ورود متقاضیان و مشتریان خدمات در دولت الکترونیک به جامعه سامانه های الکترونیکی دولت می شود، مفهوم "هویت الکترونیکی" یا همان e-Identity می باشد. همانطور که در شکل نیز مشاهده می شود، یک شهروند یا بنگاه از دید جامعه سامانه های الکترونیکی دولت، دارای ابعاد مختلف هویتی مانند هویت آموزشی، هویت انتظامی، هویت بهداشتی و ... می

باشد که زیرساخت شکل گیری تمامی این هویت ها، هویت انفرادی یا هویت سجلی شهروندان است که محل ایجاد، ثبت و نگهداری آن، سازمان ثبت احوال کشور است. در واقع سازمان ثبت احوال با ارائه "شماره ملی" در قالب کارت شناسایی ملی به عنوان کلید یکه و منحصر به فرد برای دسترسی به هویت افراد حقیقی، یکی از مهمترین گام ها را برای تحقق دولت الکترونیک در سالیان گذشته برداشته است. هم اکنون، گام مهم بعدی در راستای تکمیل زیرساخت های لازم برای تحقق دولت الکترونیک که همان تعریف مفهوم "شهروند الکترونیکی" می باشد، با اجرای پروژه کارت شناسایی ملی هوشمند توسط سازمان ثبت احوال در حال اجرا می باشد. با توجه به توضیحات ذکر شده تا کنون، شاید بتوان مهمترین هدف از اجرای این پروژه را ایجاد امکان شناسایی و اثبات هویت و ارائه خدمات گوناگون به شهروندان در فضای دولت الکترونیک عنوان کرد و کارت شناسایی ملی هوشمند را نیز به عنوان "دروازه ورود به دولت الکترونیک" معرفی نمود.

علاوه بر این موارد، سازمان ثبت احوال با ارائه خدمات الکترونیکی همچون پیگیری درخواست تغییر نام، تغییر نام خانوادگی، صدور گواهی تجرد، پیگیری وضعیت صدور کارت شناسایی ملی و رهگیری درخواست کارت شناسایی ملی ایرانیان خارج از کشور نشان داد که بخوبی توانسته است پیش زمینه ها را برای پذیرش خدمات دولت الکترونیک برای کاربران فراهم سازد و نقش بسزایی را در ارتقای جایگاه ایران در دولت الکترونیک در جهان ایفا نماید. اکنون جایگاه نظام نوین ثبت احوال در قلب خدمات مشاع زیرساخت دولت الکترونیکی کشور بسیار کلیدی و پر اهمیت است و تحقق آن یکی از شروط لازم شفافیت سایر ابعاد هویتی شهروندان و تحقق سامانه های کاربردی الکترونیکی در بستر دولت الکترونیک می باشد. سازمان ثبت احوال همچنین با ایجاد بانک اطلاعات ایرانیان گام موفق دیگری را در توسعه و پیاده سازی دولت الکترونیک برداشته است. با نظام جامع شناسایی ایرانیان که در ثبت احوال طراحی شده است، پاسخگویی به مراجع ذیصلاح قضایی از اعتماد و و اطمینان خاطر مضاعفی برخوردار شده است. اکنون ثبت احوال به عنوان یک نهاد ایجادکننده بستر و زیرساخت نقش مهمی در تحقق دولت الکترونیک ایفا می کند. این سازمان با مکانیزه کردن سیستم های ارائه خدمات خود به شهروندان توانسته است امکان ارائه خدمات نوین الکترونیکی یکسان به مردم در شهر و روستا را داشته باشد و

با سیستم های نوین الکترونیکی ، تبادل آمار و اطلاعات بسیار دقیق تر ، نقش مهمی در برنامه ریزی های کلان کشور در حیطه دولت الکترونیک داشته باشد

موانع گسترش دولت الکترونیک

از جمله مشکلات موجود بر سر راه سازمان ها در گسترش دولت الکترونیک می توان به موارد ذیل اشاره کرد :

۱- عوامل فرهنگی

ممکن است کارکنان درک کامل و درستی از دولت الکترونیک ندارند، که می توان آن ها را به دو گروه تقسیم کرد:

- گروهی که سواد کامپیوتری ندارند و از طرف دولت الکترونیک و فرهنگ مربوط به آن احساس تهدید می کنند. این گروه از کارکنان به دلیل ترسشان در مقابل هر نوع اصلاحات عصر اطلاعات مقاومت می کنند.

- کسانی که سواد کامپیوتری دارند، بدون توجه به نیاز مبرم به ایجاد هماهنگی میان فعالیتهای فناوری اطلاعات، می خواهند برنامه خود را دنبال کنند. این افراد به هیچ وجه مایل نیستند که تلاش های خود را در قالب یک برنامه اصلاحی جامع تر تعالی ببخشند و بنابراین هر نوع تلاش سازمانی با رویکرد یکپارچه سازی نسبت به اصلاحات دولت الکترونیک را تضعیف می کنند. آموزش و ایجاد زیرساخت مناسب می تواند سازمان ها را در رفع این مسئله یاری نماید.

بررسی دولت ها و مطالعات اولیه آنها برای به اجرا درآوردن طرح دولت الکترونیک نشان داده است که مشکل اصلی ایجاد و توسعه دولت الکترونیک، تکنولوژی نیست، بلکه مشکل اصلی در این است که آیا فرهنگ جامعه آمادگی پذیرش تغییرات بسیار زیادی که ایجاد خواهد شد را دارد یا خیر.

این تغییرات تأثیر اصلی خود را بر کارمندان خواهند گذاشت. برای راضی کردن عموم مردم نیز باید جامعه را متقاعد کرد که انتقال اطلاعات به قدر کافی امن هست و حریم خصوصی افراد کاملاً رعایت می شود. در ساختار سازمانی یک دولت الکترونیک، کارمندان به جای جلوگیری از خطر و ریسک در کارهای اداری به مدیریت ریسک می پردازند.

۲ - عوامل سازمانی و اداری

ساختار اداری مطلوب دولت الکترونیک در یک نظام دولتی الکترونیک، موانع و حصارهای بین سازمانی برداشته می‌شود و دولت از یک نظام بسته و محتاط به یک نظام باز که در آن نوآوری حرف اول را می‌زند تبدیل می‌شود.

در حال حاضر، ادارات دولتی دارای روابط بین سازمانی نیستند و یا اینکه این روابط ضعیف است و این به دلیل فقدان یک شبکه الکترونیکی مناسب بین آنها است. مسئولان این سازمان‌ها نیز تنها به مدیریت در حوزه درون سازمانی عادت کرده‌اند و ارتباط بین سازمان‌های مختلف می‌تواند مشکلاتی را برای آنها ایجاد کند. روش تصمیم‌گیری بالا به پایین نیز عامل دیگری است که به مشکلات مدیریتی دامن زده است.

۳ - کمبود منابع

کمبود امکانات مالی و عدم اولویت بندی در تخصیص سرمایه از جمله مسائلی است که می‌تواند بر سر راه گسترش دولت الکترونیک قرار گیرد. بکارگیری فناوری اطلاعات نیازمند سرمایه گذاری و اختصاص بودجه لازم از سوی سازمانهاست. نیاز به سرمایه گذاری عمده در زمینه دولت الکترونیک از جمله مسائل باز دارنده در جهت اشاعه فناوریهای جدید اطلاعاتی و ارتباطی در سازمانهاست. همچنین کمبود نیروی انسانی متخصص یک مشکل عمده در راه سرعت بخشیدن به روند تغییر به دولت الکترونیک به شمار می‌رود.

نتیجه گیری

برای آنکه دولت الکترونیک به صورت راهبردی در سطح سازمان های کشور مورد استفاده قرار گیرد، به برنامه ریزی دقیقی نیاز است. این برنامه ریزی شامل مطالعه عمیق در فرهنگ سازمان، توانایی سازمان، انجام تغییرات، محیط خارجی سازمان، میزان پشتیبانی مدیریت، نیازهای اطلاعاتی سازمان و راههای برآورده ساختن آنها می‌شود. همچنین باید مهارتهای موجود در سازمان در زمینه تکنولوژی اطلاعات جهت توسعه و پیاده سازی دولت الکترونیک بررسی گردند تا اطمینان حاصل گردد که نیروی انسانی مناسب و کافی برای نگهداری سیستم ها هم در بعد سخت افزار و هم نرم افزار وجود داشته باشد. بنابراین نیرو های انسانی باید در زمینه های مختلف دولت الکترونیک آموزش داده شوند.

خدمات در دولت الکترونیک بر اساس ارتباط بین جامعه مشتریان با جامعه سامانه های کاربردی الکترونیکی شکل می گیرد. روابط گوناگون میان شهروندان حقیقی و بنگاه های حقوقی با دولت، زمینه ساز ارائه انواع خدمات در بستر دولت الکترونیکی خواهد بود که باعث ایجاد مفهومی تحت عنوان "جامعه سامانه های الکترونیکی دولت" می شود. در این خصوص می توان به این نتیجه رسید که اگر کلیه دستگاه های ذیربط در ایفای نقش خود در اجرا و بکارگیری دولت الکترونیک موفق باشند و در ایجاد زیرساخت های قانونی، مالی و اجرایی و همچنین طراحی، ساخت و پیاده سازی دولت الکترونیک با یکدیگر همکاری کنند بدون شک شاهد توسعه ای پایدار در زمینه دولت الکترونیک باشیم.

فهرست منابع

۱. پروین، فرح ناز، **قانون ثبت احوال**، به انضمام دستورالعمل ها و آیین نامه های مربوطه، تهران: انتشارات مجد، چاپ سوم، ۱۳۸۹.
۲. سازمان ثبت احوال (آذر ۱۳۹۰)، **ثبت احوال دریچه دولت الکترونیک**، مجله ثبت، دوره جدید، شماره ۷، صفحه ۱۶
۳. سازمان ثبت احوال (بهمن ۱۳۹۰)، **جایگاه ایران در رتبه بندی دولت الکترونیک در جهان**، مجله ثبت، شماره ۹، ص ۷
۴. سازمان ثبت احوال (بهمن ۱۳۹۰)، **جایگاه ثبت احوال در دولت الکترونیک کلیدی است**، مجله ثبت، شماره ۹، صفحه ۱۷
۵. سازمان ثبت احوال (مرداد ۱۳۹۱)، **نقش ثبت احوال در توسعه و پیاده سازی دولت الکترونیک**، نشریه ثبت، شماره ۱۵، صفحه ۲
۶. سازمان ثبت احوال (خرداد ۱۳۹۲)، **نقش کلیدی پایگاه اطلاعات جمعیتی ثبت احوال**، نشریه ثبت، شماره ۲۵، صفحه ۵
۷. سرلک، محمدعلی و فراتی، حسن، **سیستم های اطلاعات مدیریت پیشرفته**، تهران: انتشارات دانشگاه پیام نور، جلد اول، چاپ سوم، ۱۳۹۰

8. <http://www.Sabteahval.ir>

9. <http://www.itna.ir>

10. Evans, Donna. Yen, David (2006) "Electronic Government" .
www.scienceDirect

بستر کاربردی شدن کارت هوشمند ملی

محمد قاسمی^۱، بهنام سعیدی^۲

چکیده

پروژه‌ی کارت هوشمند ملی از جمله پروژه‌هایی است که وسعت و گستردگی فراوان و زیادی در ابعاد مختلف دارد از آن جهت که هر فردی با هویت و تابعیت ایرانی در آینده دارای یک کارت هوشمند ملی خواهد شد که این کارت علاوه بر ویژگی‌های ظاهری معمول برای همه کارت‌های شناسایی، یک تراشه الکترونیکی نیز به همراه دارد و از کاربری‌های متفاوتی نیز برخوردار است و همچنین اطلاعات فرد، بر روی آن تراشه نیز ثبت شده است. تأمین امنیت تراشه مذکور، با استفاده از روش‌های رمزنگاری و بطور خاص، زیرساخت کلید عمومی انجام می‌گیرد. علاوه بر این، الکترونیکی شدن کارت، مزایای بسیاری را به همراه دارد. فراهم شدن امکان امضای دیجیتالی برای عموم مردم، همچنین تصدیق هویت افراد به شکلی مطمئن‌تر، از جمله این مزایاست. این امکانات نیز به کمک زیرساخت کلید عمومی فراهم می‌شود. به این منظور، برای تمام افرادی که تابعیت و هویت ایرانی دارند، حداقل دو زوج کلید نامتقارن تولید و برای هر یک، گواهینامه صادر خواهد شد. بدیهی است که پیچیدگی و وسعت این زیرساخت کلید عمومی که قصد دارد برای تمام افراد جامعه، گواهینامه صادر کند، بسیار گسترده و شاید بی‌نظیر است. از این رو طراحی زیرساخت مذکور، دقت و هوشمندی زیادی می‌طلبد. به همین منظور، پیش از هرگونه اقدامی به منظور طراحی این زیرساخت، تجاربی که سایر کشورها در این خصوص داشته‌اند را مطالعه می‌کنیم تا با چالش‌های مربوط به کاربردهای آن و همچنین بستر کاربردی مورد نیاز آن بیشتر آشنا شویم و از نکات مثبت آن‌ها استفاده کنیم.

کلید واژه (کارت هوشمند ملی ، هویت الکترونیک ، امضای دیجیتال ، فناوری اطلاعات)

^۱ - کارشناس آمار جمعیتی اداره کل ثبت احوال استان کرمان

^۲ - معاون فناوری اطلاعات اداره کل ثبت احوال استان کرمان Kerman_amar@yahoo.com

مقدمه

در این مبحث پیرامون بستر سازی و چرایی کاربرد کارت هوشمند ملی مطالبی ارائه می‌گردد که در ابعاد مختلف مورد بررسی نیز قرار می‌گیرد بر این اساس اولویت ویژه در تحقق طرح دولت الکترونیک، ارائه‌ی حداکثر تسهیلات برای شهروندان، همچنین ساده کردن عملیات مدیریت است. به منظور انجام این موارد، برنامه‌ای برای استقرار دولت الکترونیک در سال ۲۰۰۳ تدوین شد که طی آن قواعد اصلی طرح و خطکشی‌های مناسب به منظور اندازه‌گیری پیشرفت طرح دولت الکترونیک تعیین شد. این کارت علاوه بر ویژگی‌های ظاهری معمول برای همه کارت‌های شناسایی، یک تراشه الکترونیکی نیز به همراه دارد و از کاربری‌های متفاوتی نیز برخوردار است و همچنین اطلاعات فرد، بر روی آن تراشه نیز ثبت شده است. تأمین امنیت تراشه مذکور، با استفاده از روش‌های رمزنگاری و بطور خاص، زیرساخت کلید عمومی انجام می‌گیرد. علاوه بر این، الکترونیکی شدن کارت، مزایای بسیاری را به همراه دارد. فراهم شدن امکان امضای دیجیتالی برای عموم مردم، همچنین تصدیق هویت افراد به شکلی مطمئن‌تر، از جمله این مزایاست. این امکانات نیز به کمک زیرساخت کلید عمومی فراهم می‌شود. به این منظور، برای تمام افرادی که تابعیت و هویت ایرانی دارند، حداقل دو زوج کلید نامتقارن تولید و برای هر یک، گواهی‌نامه صادر خواهد شد که بسته به نوع کاربرد و زیر ساخت در موارد مختلف مورد استفاده امور اجتماعی و اداری قرار خواهد گرفت.

کارت هوشمند ملی و ساختار آن در دولت الکترونیک

در این مقاله زیرساخت کلید عمومی در سایر کشورها مورد بررسی قرار می‌گیرد و ارتباط آن با زیرساخت مورد استفاده در صدور کارت هوشمند ملی بررسی می‌شود. اکثر کشورهای انتخاب شده، کشورهایی هستند که در راه اندازی سیستم دولت الکترونیکی و صدور کارت هوشمند ملی، در مقایسه با سایر کشورها پیشتاز بوده‌اند. فرض بر این است که خوالندگان این مقاله آشنایی مختصری با زیرساخت کلید عمومی خواهند داشت بر این اساس مطالعه تجربیات سایر کشورها به عنوان کشورهای پیشتاز در راه‌اندازی سیستم دولت الکترونیک و کارت هوشمند ملی می‌تواند مورد استفاده قرار گیرد.

اولویت ویژه در تحقق طرح دولت الکترونیک، ارائه‌ی حداکثر تسهیلات برای شهروندان، همچنین ساده کردن عملیات مدیریت است. به منظور انجام این موارد، برنامه‌ای برای استقرار دولت الکترونیک در سال ۲۰۰۳ تدوین شد که طی آن قواعد اصلی طرح و خط‌کشی‌های مناسب به منظور اندازه‌گیری پیشرفت طرح دولت الکترونیک تعیین شد.

تاریخچه کارت هوشمند

بطور کلی کارت‌های هوشمند در سال ۱۹۷۰ اختراع و ثبت شده‌اند. چون و چراها و دلایل زیادی در مورد اینکه چه کسی این کارت‌ها را اختراع کرد وجود دارد. ولی مدعیان اصلی سه نفرند. نخست یورگن دتلوف از آلمان، دوم آریمورا از ژاپن و نفر سوم رولاند مورینو از فرانسه است که بیشتر رولاند مورینو را به عنوان مخترع این کارت‌ها قبول دارند رولاند مورینو دقیقاً در سال ۱۹۷۴ اولین کارت حافظه را اختراع کرد که برای کارت‌های هوشمند پیشرفته به کار می‌رود. در سال ۱۹۷۷ مایکل یوگن اولین میکروپروسسور که در قسمت تراشه یک کارت به کار می‌رود را اختراع کرد و یک سال بعد یوگن اولین میکروپروسسور قابل برنامه‌ریزی خودکار را اختراع کرد که در تراشه‌های دارای برنامه‌ریزی اتوماتیک به کار می‌رود و بعد از آن نیز افراد زیادی آمدند و این کارت‌ها را از لحاظ سخت‌افزاری و نرم‌افزاری توسعه دادند و به این ترتیب کارت‌های هوشمند که امروزه فراوان از آن استفاده می‌کنیم بوجود آمد.

کارت هوشمند ملی چیست؟

یک کارت هوشمند از نظر اندازه شبیه به کارت‌های اعتباری پلاستیکی (مانند کارت‌های دانشجویی، گواهینامه‌ها و...) که یک تراشه در آن کار گذاشته شده است می‌باشد. قرار دادن یک تراشه در کارت به جای نوار مغناطیسی، آن را تبدیل به یک کارت هوشمند با قدرت سرویس‌دهی در مصارف گوناگون می‌نماید. کارت‌های هوشمند از نظر اندازه و شکل ظاهری، شبیه به کارت‌های اعتباری و کارت‌های مغناطیسی معمولی هستند. ولی درون این کارت‌ها کاملاً با کارت‌های معمولی متفاوت است. کارت‌های مغناطیسی معمولی یک تکه پلاستیک ساده هستند با یک نوار مغناطیسی؛ در حالی که کارت‌های هوشمند درون خود یک ریز پردازنده دارند. قرار دادن این تراشه (چیپ میکروپروسسور) در کارت به جای نوار مغناطیسی، آن را تبدیل به یک کارت هوشمند با قدرت سرویس‌دهی در مصارف گوناگون می‌نماید این

ریزپردازنده معمولاً در زیر یک اتصال طلایی در یک طرف کارت قرار دارد. این ریز پردازنده در کارت های هوشمند در حقیقت جایگزین نوار مغناطیسی در کارت های معمولی شده است. اطلاعاتی را که روی نوار مغناطیسی کارت های معمولی وجود دارد می توان به راحتی خواند، روی آن نوشت، آن را حذف کرد و یا تغییر داد. به علت وجود همین مشکل نوار مغناطیسی محل خوبی برای نگهداری اطلاعات نیست. به همین دلیل هم برای استفاده از چنین کارت هایی نیاز به طراحی شبکه های کامپیوتری گسترده، برای تایید صحت و دریافت و پردازش اطلاعات وجود دارد. کارت هوشمند بدون نیاز به چنین امکاناتی به دلیل امنیت خود می تواند اطلاعات را در خود ذخیره کرده تا در صورت لزوم در محل های مختلف بتوان از این اطلاعات بدون نیاز به اتصال به شبکه استفاده کرد. واز یاد نبریم که در کارت های هوشمند هم میزان و تنوع اطلاعاتی که می خواهیم در تراشه اش ذخیره کنیم بستگی به توانایی چیپ داخل آن دارد

انواع کارت ها

کارت ها از لحاظ پذیرش در دستگاه کارت خوان به دو دسته تماسی و غیرتماسی تقسیم

می شوند

کارت های تماسی به طور مستقیم با کارت خوان در تماس بوده و هد دستگاه کارت خوان باید با قسمتی از کارت که حاوی اطلاعات است در تماس فیزیکی باشد و اطلاعات از طریق هد کارت خوان به آنها منتقل می شود ، لذا به طور نسبی امنیت بیشتری نسبت به کارت های غیرتماسی دارند اکثر کارت های بانکی و مالی در کشور ما اغلب از این نوع اند. از انواع این کارت ها می توان به کارت های مغناطیسی و کارت های چیپ دار اشاره کرد

کارت های مغناطیسی

اولین کارت هایی که به طور گسترده در اغلب زمینه ها از جمله تجارت الکترونیک و به عنوان کارت های بانکی و غیره مورد استفاده قرار گرفت کارت های مغناطیسی بودند. این کارت ها که با قرار گرفتن یک نوار مغناطیسی در زیر نوار سیاه رنگ بر روی کارت های پی وی سی ایجاد می شوند، و اطلاعات به صورت مغناطیسی نوشته و خوانده می شود به علت محدودیت های فیزیکی موجود حجم اطلاعاتی زیادی را شامل نمی شوند. نوار مغناطیسی روی این کارت ها از سه قسمت تشکیل شده است ۱ قسمت کارت معمولاً شامل اطلاعاتی از قبیل نام دارنده و شماره حساب شخص است و سایر اطلاعات کنترلی نیز بر روی قسمت های دیگر قرار دارد.

کارت‌های حافظه

کارت‌های حافظه در حقیقت کارت‌های چیپ داری هستند که تنها از یک حافظه تشکیل شده‌اند، که این حافظه می‌تواند غیر قابل شارژ یا با قابلیت شارژ نیز باشد. به علت عدم وجود پردازنده کنترلی امنیت این کارت‌ها کمتر از کارت‌های هوشمنداست. این کارت‌ها برای استفاده در پارکومترها مصرف می‌شوند

کارت‌های هوشمند

یکی دیگر از انواع کارت‌های چیپ‌دار، کارت‌های هوشمند است (موضوع مورد نظر ما) که معمولاً متشکل از پردازنده‌ای جهت انجام امور کنترلی، حافظه‌ای فقط خواندنی شامل سیستم عامل کارت (ماسک) و حافظه‌ای تا ۶۴ کیلوبایت جهت استفاده هستند. به علت وجود برنامه‌های کنترلی موجود و ساختار موجود در آنها ضریب امنیتی این کارت‌ها بسیار فراتر از کارت‌های مغناطیسی و دیگر کارت‌ها است. کارت‌های هوشمند از لحاظ ساختار داده‌ای موجود در آنها به دو دسته کارت ثبت اطلاعات و برنامه کاربردی تقسیم می‌شوند.

کارت‌های غیرتماسی

در کارت‌های غیرتماسی انتقال اطلاعات و تمامی ولتاژهای مورد نیاز به صورت بی‌سیم از طریق سیگنال‌های RF (فرکانس‌های رادیویی) و روش‌های تزویج القایی صورت می‌گیرد. سیستم‌های RFID در ابتدا برای مسیریابی، تشخیص موقعیت اجسام و مکان سنجی استفاده گردید و بر حسب مسافت و برد لازم دو نوع غیرفعال و فعال به وجود آمد که تفاوت اصلی در این موارد وجود باتری (منبع تغذیه) در نوع فعال برای افزایش طول برد بود.

کاربرد های کارت هوشمند

در هر کشوری علاوه بر شناسنامه، کارت‌های شناسایی متعددی به عنوان مدرک تأیید هویت و گاه تأیید صلاحیت، برای شهروندان صادر می‌شود که از آن جمله می‌توان به کارت کارمندی، گواهی‌نامه و گذرنامه اشاره کرد. یکی از ملزومات تحقق دولت الکترونیک تبدیل این کارت‌ها از شکل غیر الکترونیک به نوع الکترونیک آن است، یعنی برای هر شهروندی در دولت الکترونیک، لازم است به ازای هر کارتی که امروز دارد یک کارت الکترونیکی جایگزین آن صادر

شود و اساساً این کارت ها برای نگهداری هویت افراد در زمینه های مختلف به کار می رود اگر بخواهیم درباره همه کارت های موجود بحث کنیم از حوصله این مقاله مختصر خارج می شود به همین دلیل ما به برخی از این کارت ها که کاربرد بیشتر دارند اشاره می کنیم:

کارت پزشکی

با کارت های هوشمند، اطلاعات پزشکی و سایر اطلاعات مربوط به بیماریهای اشخاص همچنین اطلاعاتی راجع به سوابق پزشکی و دارویی و گروه خونی و سایر مشخصات پزشکی افراد در قسمت مشخصی از کارت با سطح دسترسی معین ، همچنین اطلاعات مربوط به بیمه افراد در کارت ذخیره می گردد

اطلاعات تحصیلی

اغلب دانشگاه ها هم اکنون یک کارت هوشمند دانشگاهی را برای تبادل تمامی اطلاعات دانشگاهی به کار می برند. سوابق تحصیلی ، اطلاعات مالی ، صورتحسابی ، اطلاعات کتابخانه ، ژتون های غذا و غیره همگی در یک کارت هوشمند قرار می گیرد که می تواند به صورت موثر، اطلاعات مذکور را دربرداشته باشد. این کارت، یک محیط بدون پرداختی را در محیط دانشگاه فراهم می آورد که دانشجویان از این کارت به علت راحتی از آن استفاده می کنند.

فعالیت های اداری ، دولتی

کارتهای هوشمند این امکان را برای افراد فراهم می کند که افراد مختلف یا با مراجعه حضوری و یا با استفاده از کارت خوان یا با استفاده از کارتهای بدون تماس و با استفاده ازسایت مربوط به اداره سازمان موردنظر، اطلاعات و درخواست خود را به آن سازمان ارائه کنند تا فعالیت درخواستی فرد باتوجه به اطلاعات مندرج در کارت هوشمند انجام پذیرد

اطلاعات شناسایی، هویتی و تابعیتی

با استفاده از کارت های هوشمند، اطلاعات شناسایی افراد در داخل آنها ثبت می گردد و در صورت نیاز در اختیار افراد یا سازمان های مربوطه قرار داده می شود. این اطلاعات می تواند شناسنامه ، کارت های شناسایی ، گذرنامه و... را شامل شود. در حال حاضر در کشور ما نیز این نوع کارت ها با عنوان کارت ملی هوشمند در مرحله صدور قرار دارد و احتمالاً تا چند سال دیگر جایگزین شناسنامه های ما شوند که این خود شروع بسیار جالبی برای دولت الکترونیکی خواهد

بود

کارت موبایل

یکی از آشنا ترین نوع کارت های هوشمند همین سیم کارت هایی هستند که همه ما می شناسیم که تحولی عظیم در صنعت ارتباطات ایجاد کرده که به نظر میرسد باید در این قمت خیلی توجه شود چرا که توسط یک موبایل که کارت خوان همیشه همراهی است می توان بیشتر این کارت ها را اعم از کارت شناسایی و کارت معافیت و کارت پزشکی و موارد دیگر را تنها در یک سیم کارت جمع کرد

کارت های اعتباری

اطلاعات دیگری که می تواند در کارت های هوشمند وجود داشته باشد، اطلاعات بانکی است که هر فرد می تواند اطلاعات مربوط به بانک های مختلف را به همراه اطلاعات اعتباری فروشگاه های مختلف در آن نگهداری کرده و مورد استفاده قرار دهد. به عنوان مثال ، شماره حساب فرد، میزان موجودی و همچنین سایر اطلاعات می تواند در کارت هوشمند ذخیره شده و مورد استفاده قرار گیرد. در حال حاضر بیشترین کاربرد کارت های هوشمند در این بخش است و عملا در تبادلات مالی تحولی بزرگ ایجاد کرده است و ابزار اصلی پول الکترونی محسوب می شود در ایران هم چند سالی است که در این زمینه بسیار فعالیت می شود .

کارت خودرو

این کارت برای بکارگیری فناوری های نو در زمینه عرضه خدمات فروش و پس از فروش به مشتریان خودرو ارایه می شود و با این کارت تبادل اطلاعات کاملتری را با ماشین و مشتری برقرار می کنیم. البته در کشور های پیشرفته این اطلاعات این کارت ها در کارت های دیگری از جمله کارت سوخت ادغام شده است ولی در حال حاضر در ایران این کارت در حال طراحی جداگانه ای است که این طرح توسط شرکت ایران خودرو در حال انجام می باشد

کارت سوخت

یکی از کاربرد های کارت هوشمند استفاده از آن در سیستم فروش سوخت در جایگاه های عرضه سوخت است که این کاربرد بیشترین سود اقتصادی را برای دولت و بیشترین راحتی را برای مردم دارد که کار خرید سوخت آنها براحتی انجام میگیرد در حال حاضر در کشور ما نیز طرح کارت هوشمند سوخت با هدف استفاده بهینه سوخت و جلوگیری از قاچاق سوخت در حال اجرا است .سیستم کارت هوشمند سوخت، کلیه عملیات و کنترل عرضه سوخت را با

استفاده از کارت های هوشمند مکانیزه کرده و بستر مناسبی را برای اجرای فعالیت های متعدد، از جمله امکان دسترسی دقیق به آمار و ارقام سوخت مصرفی کلیه وسایط نقلیه بنزین سوز و گازوئیل سوز در سراسر کشور و در بخش های مختلف مصرف- دولتی، خصوصی، عمومی- فراهم می آورد و با هدف مدیریت بر مصرف بهینه سوخت در کشور این روند آغاز می شود به هر حال کارت هوشمند کاربرد های گوناگونی دارد که در هر کشور ممکن است این کاربرد ها متفاوت باشد به همین دلیل فقط انهایی که ممکن است در بیشتر کشور ها مشترک است را بر شمرده و مختصراً بیان شد.

اهمیت پروژه‌ی کارت هوشمند ملی

به منظور اجرای پروژه‌ی کارت هوشمند ملی در ایران، فازهای مختلفی در نظر گرفته شده است. اولین فاز این پروژه انجام مطالعات تطبیقی بر کشورهای همسایه و حوزه‌ی خلیج فارس در زمینه‌ی کارت هوشمند ملی است. ناگفته پیداست که قدم اول به منظور توسعه‌ی سیستمی که قبلاً در مناطق دیگر در حال اجرا یا اجرا شده است، مطالعه‌ی روش‌ها، فعالیت‌ها، استراتژی‌های راهبردی در زمینه‌ی اجتماعی و فنی، فناوری‌های مورد استفاده و نحوه‌ی اجرای آن‌ها است. هدف مقاله حاضر نیز بررسی این موارد به نحو دقیق‌تر است؛ بررسی استراتژی دولت الکترونیک، خدمات ارائه شده به صورت الکترونیک، تاریخچه‌ی فعالیت‌های انجام شده در این زمینه، مشخصات فنی کارت و شناخت کارفرمایان و پیمانکاران پروژه در کشورهای مختلف محتوای اصلی این بخش را تشکیل می‌دهد و در حد امکان سعی شده به مهمترین و اصولی ترین منابع و مسایل مرتبط با کارت هوشمند ملی تاکید گردد که عموماً شامل موارد زیر خواهند بود :

- سایت‌های وزارت کشور یا سازمان‌های معادل
- پورتال‌های دولت الکترونیک
- سایت‌های رسمی پیمانکاران پروژه
- سایت سازمان ثبت احوال کشور
- ماهنامه کارت هوشمند ملی
- حرکت به سمت دولت الکترونیک

با بزرگ شدن جوامع به لحاظ اندازه و گستردگی جمعیت، نیاز به سیستمی به منظور مدیریت اطلاعات افراد و ارائه خدمات به روشی ساده‌تر، راحت‌تر و در دسترس عموم انکارناپذیر است. دولت الکترونیک در هر دو حوزه‌ی مدیریت اطلاعات افراد و ارائه‌ی خدمات، زیرساخت مناسبی را فراهم می‌آورد تا کارها ساده‌تر و با امنیت بالاتری انجام شود.

با طرح سؤالات زیر می‌توان انگیزه‌ی حرکت به سمت دولت الکترونیک را در ذهن ایجاد کرد. هزینه‌هایی که می‌تواند با کارت هوشمند ملی و دولت الکترونیک از آن‌ها جلوگیری شود:

- میزان هزینه‌های ناشی از جعل مدارک هویتی
- میزان هزینه‌ی تبادل مکاتبات اداری درون دولت
- هزینه صرف زمان تبادل مکاتبات
- هزینه مسافرت های درون شهری
- هزینه انجام امور بانکی و اقتصاد

این موارد صرفاً تعدادی از انبوه مواردی است که وجود دارد. نکته مشترکی که در تمام موارد بالا مشاهده می‌شود، هدر دادن زمان، هزینه، فشارهای روحی و خستگی است. با وجود زیرساخت دولت الکترونیک، امکان ارائه‌ی خدمات به روشی سریع‌تر، با امنیت بیشتر و به دور از هیاهوی شهر صرفاً با جابه‌جایی در فضای مجازی وب فراهم می‌شود. به این ترتیب زمان مفید اشخاص افزایش می‌یابد، هزینه‌های اضافی حذف می‌شوند و افراد تمامی خدمات را با دسترسی به پورتال دولت الکترونیک از طریق کامپیوتر شخصی خود در منزل دریافت خواهند کرد.

این مزایایی بود که برای شهروندان فراهم می‌شود. برای خدمات دهندگان از جمله مراکز دولتی یا غیر دولتی نیز مزایایی فراهم می‌شود. شاید یکی از مهم‌ترین این مزایا کاهش تمرکز بر ارائه خدمات، تمرکز بیشتر بر مدیریت خدمات و افزایش سطح خدمات است. انگیزه‌ی کشورهای مختلف برای اجرای کارت هوشمند انگیزه‌ی کشورهای مختلف به منظور اجرای پروژه‌ی کارت هوشمند ملی بنا بر اظهارات خودشان، طیف وسیعی را پوشش می‌دهد. از جمله این موارد انگیزه‌هایی برای کاربردهای مختلف شناسایی و تصدیق هویت از جمله گیت‌های الکترونیک، پرداخت هزینه پارکینگ و حمل و نقل عمومی، پرداخت قبوض، رأی‌گیری، اطلاعات پزشکی، گواهینامه‌ی رانندگی و تراکنش‌های الکترونیکی و اینترنتی دارد. البته این به این معنا نیست که تمام این موارد را در کارت خود اجرا کرده است. علاوه بر

زیرساخت‌هایی که برای کاربردهای کارت استفاده میشود، این امکان را فراهم می‌کند تا کارت در آینده در گیت‌های الکترونیک کشورهای مختلف به عنوان سند مسافرتی نیز استفاده شود. از جمله دیگر دلایل که به منظور اجرا و توسعه‌ی مرکز داده قابل ذکر است شامل مدرن کردن سیستم ثبت ملی، افزایش سادگی و سرعت در فرآیندهای مدیریتی، ارائه‌ی خدمات بهتر، تأمین بهتر امنیت داخلی و ساخت بستری برای ارائه‌ی خدمات الکترونیکی است. دلیل دیگر از پیاده‌سازی کارت هوشمند ملی مواردی از قبیل افزایش خدمات به شهروندان، کاهش جعل مدارک شناسایی، ایجاد زیرساخت مناسب برای دولت الکترونیک، همچنین استفاده از اسناد شناسایی چند منظوره و با دوام است.

همچنین مواردی مشابه موارد بالا به عنوان سایر انگیزه‌ی اجرای کارت هوشمند ملی در سایر کشورها قابل ذکر خواهند بود از آن جمله می‌توان به تصدیق هویت برای خدمات عمومی و مالی، تأیید شایستگی برای خدمات، محافظت از حریم خصوصی افراد، به همراه داشتن یک کارت به جای چندین کارت، تسهیل ارائه‌ی خدمات دولتی و گنجاندن پرونده‌های پزشکی، کاهش خطاهای انسانی در شناسایی و تصدیق هویت، وجود سطوح دسترسی مختلف امنیتی برای دسترسی به اطلاعات کارت، حذف نیاز به حضور متقاضی خدمات در مراکز خدماتی، انجام تراکنش‌های مالی در سطح اینترنت یا هر محیط الکترونیکی دیگر اشاره کرد.

از طرفی میتوان موارد حذف، جعل و تقلب کارت شناسایی، شناسایی هویت به صورت آنلاین و آفلاین، به همراه داشتن یک کارت به جای چندین کارت، تقویت عرقِ ملی در شهروندان، حفاظت از شناسایی افراد در مقابل تقلب و سوء استفاده تبه‌کاران از هویت آن‌ها و تسهیل ارائه و استفاده از خدمات به صورت الکترونیکی و همچنین استفاده کارت به عنوان سند شناسایی در مرزها و مسافرت بین کشورها به عنوان دلایل متفاوت برای اجرا و صدور کارت هوشمند ملی نام برد. در همین راستا همچنین استفاده از پایگاه داده‌ی جامعی که در پی توسعه‌ی کارت هوشمند ملی ایجاد می‌شود، کاهش هزینه‌های مدیریت داده را به دنبال خواهد داشت نیز اشاره داشت.

با توجه به آنچه گفته شد و تائید همه موارد فوق الذکر و تاکید بر اهمیت همه موارد مطروحه دلیل اصلی برای اجرای پروژه‌ی کارت هوشمند ملی، فراهم آوردن زیرساخت مناسب به منظور خدمات الکترونیکی و حرکت به سمت ایجاد دولت الکترونیک و جامعه‌ی اطلاعاتی

خواهد بود به عبارتی کارت هوشمند ملی ، کلید ورود و دریافت خدمات الکترونیکی در دولت الکترونیک بشمار میرود .

در مالزی، طرح کارت هوشمند ملی با هدف توسعه‌ی پلتفرمی (plat form) واحد، برای یک کارت چند منظوره که بتواند به دولت و سرویس دهنده‌های خصوصی این امکان را بدهد که در اجرای کارت هوشمند، بدون انجام کارها و هزینه‌های تکراری کمک کند. این کارت در حال حاضر کاربردهای مختلفی دارد. اما میزان استفاده از آن میان مردم، مسئله‌ی دیگری است. این کاربردها عبارتند از: شناسه‌ی ملی، گواهینامه‌ی رانندگی، اطلاعات گذرنامه، اطلاعات سلامت و زیرساخت کلید عمومی.

فعالیت‌های کره‌ی جنوبی در حرکت به سمت دولت الکترونیک و کارت هوشمند ملی قبل از سال ۲۰۰۰ آغاز شد. اما به علت پاره‌ای از مشکلات نظیر مقابله با گروه‌های مدافع و حفظ حریم شخصی، این فعالیت‌ها بی ثمر ماند. استفاده از فناوری اطلاعات به منظور افزایش کارایی دولت، ایجاد شفافیت در فعالیت‌های دولت، تسهیل دسترسی به خدمات، بهبود خدمات، افزایش کیفیت زندگی شهروندان و محرومان و در نهایت گسترش مشارکت عمومی در فعالیت‌های کشور، دلایل اصلی کره به منظور پیشبرد طرح دولت الکترونیک است. کره‌ی جنوبی در طرح کارت هوشمند ملی کاربردهای مختلفی را مطرح کرده است. شناسایی با استفاده از گواهینامه‌ی دیجیتال و بیومتریک، در کاربردهایی نظیر دولت الکترونیک بخش خصوصی، خدمات رفاه اجتماعی و رأی‌گیری، همچنین کاربرد آن در ارائه‌ی خدمات عمومی نظیر گواهینامه‌ی رانندگی، کارت مهاجرت، کارت اتباع خارجی، بیمه‌ی سلامت و کارت پرداخت، استفاده در بخش حمل و نقل عمومی، از جمله انگیزه‌ها و اهداف کره به منظور پیگیری طرح کارت هوشمند ملی در این کشور بوده است.

طرح دولت الکترونیک سنگاپور، در سال ۲۰۰۰، با پنج موضوع کلیدی مطرح شد. این پنج موضوع شامل بازسازی دولت، ارائه‌ی خدمات الکترونیکی، پیشرو بودن در راهبرد تشخیص و پاسخ، استفاده از ICT برای ظرفیت‌سازی و استعداد سازی به منظور جهش در ارائه‌ی خدمات با کیفیت و نوآوری است. به همین منظور، یک شناسه‌ی کاربری و کلمه‌ی عبور موسوم به Sing Pass به هر یک از شهروندان اختصاص داده شد تا به خدمات الکترونیکی دسترسی یابند.

از کارت ملی سنگاپور، به عنوان مدرک شناسایی در مراکز دولتی و غیر دولتی برای انجام مراحل مختلف اداری و تراکنش‌های تجاری نظیر باز کردن حساب بانکی یا درخواست محموله‌ی پستی در اداره‌ی پست استفاده می‌شود. هم‌چنین کارت شناسایی برای اتباع خارجی به عنوان مکملی در کنار گذرنامه به منظور کسب جزئیات بیشتر از فرد، مانند آدرس اقامت، استفاده می‌شود.

اهداف اصلی دولت الکترونیک از دیدگاه تغییر مدیریت در ژاپن از منظرهای مختلفی بررسی می‌شود: ارائه‌ی تسهیلات به شهروندان و بنگاه‌ها، شفافیت فعالیت‌های دولت، مدیریت با انعطاف‌پذیری و هماهنگی بیشتر، افزایش کارایی دولت، ترویج کار بدون کاغذ و ترویج اشتراک اطلاعات با استفاده از سیستم‌های پایگاه داده از جمله این موارد است.

ژاپن کشور پیری است و با کاهش تدریجی نیروی فعال و کارآمد در جامعه مواجه است، طبیعتاً این امر موجب کاهش تولید نقدینگی و افزایش هزینه‌های تأمین اجتماعی خواهد شد. ژاپنی‌ها معتقدند با استفاده از ICT به طور غیر مستقیم می‌توانند این مسئله را حل کنند. به این ترتیب در بحث مراقبت از سلامت الکترونیکی و دولت الکترونیک سرمایه‌گذاری کردند. ظاهراً طرح دولت الکترونیکی برخلاف طرح سلامت الکترونیکی کامل شده است.

طرح دولت الکترونیک هنگ کنگ در قالب استراتژی Digital ۲۱ تعریف می‌شود. این استراتژی هر سه سال یکبار به روز رسانی می‌شود و اهدافی هم چون تسهیل اقتصاد دیجیتال، ترویج فناوری و نوآوری، تبدیل هنگ کنگ به یک هاب برای همکاری‌های فنی و تجاری، استقرار نسل‌های بعدی خدمات عمومی و ایجاد جامعه‌ی اطلاعاتی را دنبال می‌کند. انگیزه‌ی اصلی هنگ کنگ به منظور اجرای کارت هوشمند ملی، جلوگیری از مهاجرت‌های غیر قانونی است. اما از این زیرساخت در موارد دیگری نیز استفاده کرده است. کاربردهای هم‌چون امضای دیجیتال، دسترسی به تسهیلات کتابخانه‌های عمومی، تراکنش‌های الکترونیک امن روی اینترنت و خدمات با کیفیت دیگری که در آینده عرضه خواهد شد. در کل انگیزه‌هایی هنگ کنگ را برای اجرای طرح کارت هوشمند ملی می‌توان در افزایش امنیت، ارائه‌ی تسهیلات بیشتر، افزایش کیفیت خدمات و انجام مسافرت‌های سریع‌تر (تسریع ترخیص مسافر در مرزها) خلاصه کرد. شایان ذکر است، برخلاف انگلیس که با مشکلات عدیده‌ای در اجرای کارت

الکترونیکی ملی مواجهه بوده است، هنگ کنگ که مدت‌ها مستعمره‌ی انگلیس بود، تا به امروز مشکلی در رابطه با اجرا و استفاده از کارت هوشمند ملی نداشته است.

تایلند اهداف مختلفی را از اجرای پروژه‌ی دولت الکترونیک دنبال می‌کند، از جمله: بهبود ارائه‌ی خدمات الکترونیکی، مدیریت عمومی و افزایش ارتباط و همکاری بین بخش‌های مختلف دولتی.

تایلند به دلایل مختلفی قصد دارد کارت ملی را به کارت هوشمند تغییر دهد. دلایلی نظیر: مسایل سرقت، جعل هویت افراد و شناسه‌های اشتباه یا چندین شناسه برای یک نفر به علاوه، کارت‌های هوشمند جدید قادر است چند کاربرد را در خود نگه دارد. مثلاً هم به عنوان کارت شناسایی سنتی ایفای نقش کند، هم به عنوان کارت شناسایی دانش‌آموزی (دانشجویی) و هم به عنوان کارت شناسایی دولتی کاربرد داشته باشد.

مقاله حاضر به مطالعه‌ی دولت الکترونیک و کارت هوشمند در منطقه‌ی خاور دور می‌پردازد که در واقع کشورهای این منطقه در این زمینه در جهان پیشرو بوده‌اند و از تجربیات آن‌ها می‌توان هم در زمینه ساختار دولت الکترونیک و هم در تولید و صدور کارت هوشمند استفاده کرد. کشورهای این منطقه که بررسی شده‌اند، عبارتند از: تایلند، ژاپن، کره‌ی جنوبی، مالزی و هنگ‌کنگ.

ضرورت کارت هوشمند ملی

امروزه با گسترش کاربرد کارت هوشمند در بسیاری از کشورها به‌منظور کاربردهای هویت و پرداخت، برخی از سازمان‌های بین‌المللی و منطقه‌ای با هدف یکسان‌سازی و هماهنگ‌سازی استانداردها و پیش‌نیازهای اصلی کارت هوشمند (به‌ویژه هویت) در کشورهای مختلف از قاره‌های مختلف به وجود آمده‌اند تا افراد (تجّار و گردشگران) برای نقل و انتقال راحت در کشورهای مختلف بتوانند از کارت هویت ملی خود استفاده کنند.

در حوزه‌ی کشورهای اروپایی و اتحادیه‌ی اروپا، از چند سال پیش، بحث استفاده از کارت‌های هوشمند مطرح بود، این کشورها به تدریج به ایجاد زیرساخت‌های لازم و استفاده از این کارت‌ها روی آورده‌اند. تا امروز حدود نیمی از ۲۷ کشور عضو اتحادیه‌ی اروپا از کارت هوشمند ملی بهره گرفته‌اند و پیش‌بینی می‌شود در آینده بر اساس برنامه‌ریزی‌های به‌عمل آمده در اتحادیه‌ی اروپا، تعداد کشورهای استفاده‌کننده از کارت هوشمند ملی افزایش یابد.

با توجه به پیشرفت‌های چشمگیر دولت الکترونیک و خدمات آن در کشورهای اروپایی، در اکثر این کشورها، کارت‌های هوشمند الکترونیکی رواج گسترده‌ای داشته است. کاربردهای این کارت‌ها در سطوح وسیعی از جمله کارت سلامت و تأمین اجتماعی، گواهینامه‌های الکترونیکی، کارت الکترونیکی برای استفاده‌های عمومی هم‌چون حمل و نقل عمومی، محیط‌های آکادمیک و دانشگاهی، خرید در فروشگاه‌ها و غیره قابل توصیف است.

در این بخش به طور تفصیلی به رویکرد کشورهای اروپایی، در استفاده از کارت‌های هوشمند و کارت‌های شناسایی الکترونیکی پرداخته شود و دلایل استفاده کشورهای اروپایی از کارت هوشمند ملی بیشتر مورد تأکید قرار می‌گیرد که وضعیت استفاده از سیستم‌های مدیریت هویت الکترونیکی، کاربردها و موارد استفاده این کارت‌ها که در سایر کشورها از اهمیت بالایی برخوردار است باید مورد توجه و تأکید واقع شود و در نهایت توجه به زیرساخت‌های فنی و حقوقی و قانونی مورد نیاز در پروژه کارت هوشمند ملی باید به عنوان پیش نیاز و مقدمه اجرای پروژه نیز جایگاه خاص خود را دارد که نباید فراموش شود.

فناوری اطلاعات و کارت هوشمند ملی

بسیاری از اقتصاددانان و متخصصین بر این عقیده‌اند که انقلابی مشابه انقلاب صنعتی به وقوع پیوسته که جهان را وارد عرصه اطلاعات ساخته و بسیاری از جنبه‌های اقتصادی، اجتماعی و فرهنگی حیات بشر را دستخوش تحولی عظیم نموده است. رشد روزافزون فن‌آوری بخصوص فن‌آوری اطلاعات (IT) در جهان، موانع و مشکلات زمانی و مکانی مربوط به امور تجاری را کاهش داده است و دسترسی عمومی مردم به اینترنت باعث شده امکان تجارت و کسب و کار از طریق اینترنت و یا به عبارتی تجارت الکترونیکی و کسب و کار الکترونیکی از جایگاه ویژه‌ای در کشورهای توسعه یافته برخوردار شود.

در سال‌های اخیر کشورهای توسعه یافته با کنار گذاشتن تدریجی تجارت سنتی مبتنی بر کاغذ و مبادله فیزیکی اسناد، به شیوه تجارت الکترونیکی روی آورده‌اند. روش تجارت الکترونیکی معروف به تجارت بدون کاغذ، صرفه‌جویی در زمان، هزینه‌ها و نیروی انسانی را به دنبال داشته و شاخص‌های بهره‌وری را افزایش داده است اما این شیوه هنوز در کشور ما جایگاه خود را به دست نیاورده است. یکی از مصادیق تجارت الکترونیک، دولت الکترونیک بوده که در این بخش به آنها پرداخته می‌شود که تبیین مفاهیم و تعاریف رایج و پرکاربرد در حوزه دولت

الکترونیک اجتناب ناپذیر مینماید ضمن اینکه توصیف وضعیت کنونی دولت الکترونیک در کشورهای عضو اتحادیه اروپا به عنوان کشورهای پیشرو در حوزه برخورداری از ایجاد و دریافت خدمات دولت الکترونیک و استفاده از آن نیز دور از انتظار نخواهد بود همچنین ضمن بیان ویژگی‌ها و وضعیت عمومی کشورهای مذکور و توصیف شاخص‌های جامعه اطلاعاتی و ساختار دولت الکترونیک و همچنین زیرساخت‌های آن بسیار مفصل میباشند که توضیح در مورد بخش‌ها و سازمان‌های مرتبط با دولت الکترونیک، چه به لحاظ آماده‌سازی زیرساخت‌ها و چه به لحاظ بهره‌مندی از مزایای آن به دلیل گستردگی و تفصیل در این مقاله نمیگنجد و نیاز به گزارشی جداگانه دارد لذا توصیف وضعیت دولت الکترونیک در ایران، براساس گزارشات پیاده‌سازی این سیستم همچنین قوانین تصویب شده در این زمینه در راستای پیاده‌سازی دولت الکترونیک و اسناد معتبر موجود بایستی بررسی گردند تا تمامی زوایای مورد نیاز در ایجاد دولت الکترونیک مورد کنکاش قرار گرفته باشند

براساس یکی از تعاریف دولت الکترونیک که آن را «استفاده آسان از فناوری اطلاعات به منظور توزیع خدمات دولتی به صورت مستقیم و شبانه‌روزی به مشتری (شهروندان) می‌داند، این مقاله و مطالب آن، می‌تواند به عنوان پیش زمینه‌ای برای استفاده از کارت هوشمند ملی بعنوان ابزار فناوری اطلاعات کلیدی مهم در راستای ارائه خدمات دولت به شهروندان جهت ورود به دولت الکترونیک مورد استفاده قرار بگیرد

نتیجه گیری

رشد جمعیت و توسعه روز افزون فناوری اطلاعات و ارتباطات از مشخصه های بارز قرن بیست و یکم است. گسترش فناوری اطلاعات و استفاده از سامانه‌های شبکه‌ای یکپارچه رایانه‌ای، تغییر و تحولات بسیاری را در زمینه‌های مختلف اقتصادی، اجتماعی، و سازوکارهای ارائه خدمات عمومی و دولتی فراهم ساخته است. این تحولات تا آنجا پیش رفته است که اغلب کشورها سازو کارهای مدیریتی و خدمات‌رسانی را در بستری تحت عنوان دولت الکترونیک دنبال کرده‌اند و با ایجاد زیرساخت‌های لازم در پی آنند که دسترسی درون خطی آسان و امن مردم و مؤسسات به انواع خدمات عمومی و دولتی را با هزینه کمتری فراهم نمایند؛ به طوری که نیاز مراجعه حضوری آنها به دستگاه‌های خدمت دهنده به حد اقل ممکن کاهش یابد. در همین زمینه چالش مهم چگونگی و چرایی نیاز به شناسایی و تصدیق هویت درخواست کنندگان

خدمات در نظام سنتی که بر مراجعه حضوری مردم به دستگاه‌ها و مقایسه اسناد سجلی و افراد متکی بود، در فضای الکترونیکی جدید از چه میزان کارایی لازم برخوردار است. به همین دلیل، در بیشتر کشورها برنامه‌های جامعی برای ایجاد امکانات شناسایی و تصدیق هویت الکترونیک در دستور کار قرار گرفته است و هم‌اکنون تعدادی از آنها از کارت‌های شناسایی هوشمند استفاده می‌کنند. این کارت‌ها که از نوع پلی‌کربنات است، حامل تراشه برای ذخیره‌سازی اطلاعات سجلی، عکس و بیومتریک است و امکانات امنیتی متعدد و متنوعی نیز در آنها تعبیه شده است. سازمان ثبت احوال کشور که دستگاه مسؤول ایجاد و حفظ اسناد هویتی مردم است، طی دو دهه اخیر با ایجاد سامانه جامع مکانیزه ثبت احوال، پایگاه متمرکز اطلاعات جمعیتی و صدور کارت شناسایی حاوی شماره ملی، علاوه بر متحول ساختن نظام شناسایی و تصدیق هویت آحاد مردم، زیرساخت اصلی اصلاح سامانه‌های انسانی در نظام‌های اداری، آموزشی، درمانی، اقتصادی، اجتماعی و ... را نیز فراهم ساخته است.

قانون برنامه پنجم کشور، در جهت تحقق دولت الکترونیک، مسؤولیت کارت هوشمند ملی را که زیرساخت شناسایی و تصدیق هویت آحاد مردم در فضای دولت الکترونیک محسوب می‌شود به سازمان ثبت احوال کشور محول کرده است و این سازمان نیز در جهت تحول مستمر سامانه خدمات هویتی خود، طی دو سال اخیر اقدامات مؤثری را به عمل آورده و هم‌اکنون نیز برنامه ایجاد سامانه و صدور کارت هوشمند ملی را با جدیت دنبال می‌کند که در استان قم این پروژه عملیاتی شده است ضمن اینکه در سایر استان‌ها بررسی مقدمات و تامین پیش‌نیازها و تجهیزاتی اجرای آن در دستور کار قرار گرفته شده و عملیات میدانی و اجرایی این پروژه مهم و عظیم در دست اجرا می‌باشد.

منابع :

کارت هوشمند ملی، تجربه کشور ژاپن در دولت الکترونیک تألیف و گردآوری : مرکز آموزش و حوزه کارت هوشمند ملی.

کارت هوشمند ملی، تجربه کشورهای حوزه خلیج فارس و خاورمیانه در دولت الکترونیک تألیف و گردآوری : مرکز آموزش و حوزه کارت هوشمند ملی

کتاب : کارت هوشمند ملی، تجربه کشورهای خاور دور در دولت الکترونیک تألیف و

گردآوری : مرکز آموزش و حوزه کارت هوشمند ملی

کتاب : نقش کارت هوشمند ملی در ارائه خدمات دولت الکترونیک در کشورهای عضو اتحادیه اروپا تألیف و گردآوری : مرکز آموزش و حوزه کارت هوشمند ملی

کتاب : کارت هوشمند ملی، ساختار و نقش آن در دولت الکترونیک تألیف و گردآوری : مرکز آموزش و پژوهش و حوزه کارت هوشمند ملی

وب سایت سازمان ثبت احوال کشور

ماهنامه های کارت هوشمند ملی

مطالعات کتابخانه ای