سيستم‌هاي برنامه‌ريزي منابع سازماني، چالش‌ها و مشکلات امنيتي، راهکار پيشنهادي

سيد مهدي روح‌الاميني
دانشجوي کارشناسي ارشد، دانشگاه علم و صنعت ايران، مرکز آموزش الکترونيکي
طراح ارشد سيستم، شرکت ملي صنايع مس ايران
Rooholamini@nicico.com

محمد عبدالهي ازگمي
استاديار، دانشگاه علم و صنعت ايران، دانشکدة مهندسي کامپيوتر
Azgomi@iust.ac.ir

چکيده:

امروزه، تمامي سيستم‌هاي برنامه‌ريزي منابع سازماني، سازوکارهاي امنيتي را در شکل‌هاي مختلفي ارائه مي‌کنند ولي همچنان مسائل امنيتي متعددي در شکل‌هاي مختلف در آنها ديده مي‌شود. اين مشکلات، در محصولات مختلف و از کسب‌وکاري تا کسب‌وکاري ديگر متفاوت است. استفادة سازمان‌ها و صنايع متعدد از بسته‌هاي نرم‌افزاري يکسان، مستلزم انعطاف زياد در نرم‌افزار است و ممکن است تغييرات وسيعي به‌منظور استفادة همه‌جانبه از اين سيستم‌ها، توسط عرضه‌کنندگان آنها صورت پذيرد. در حال حاضر، پياده‌سازي بخش امنيت ERP[1]، در مرحلة دوم و پس از پياده‌سازي فرآيندهاي کسب و کار صورت مي‌گيرد که در بسياري موارد و به‌علل مختلف، اين مرحله از کار کمرنگ مي‌شود. مشکل موجود ديگر، پياده‌سازي بخش امنيت، به‌صورت متمرکز است که معضلي بزرگ به‌شمار مي‌رود. پياده‌سازي امنيت متمرکز، منوط به داشتن تيمي مشرف بر کل فرآيندها و حوزة کار است که علاوه بر مشکل پيدا کردن چنين تيمي، از لحاظ امنيتي نيز صحيح نخواهد بود.

در اين مقاله سعي شده است مشکلات امنيتي برخي سيستم‌هاي ERP، از طريق مطالعة موردي، بيان شود. سپس راهکاري مبتني بر مفهوم مالکيت اطلاعات[2] ارائه شود که پياده‌سازي واقعي و استفاده از اين راهکار مي‌تواند در حذف يا کاهش مشکلات اشاره شده، تأثير به‌سزائي داشته باشد.

واژه‌هاي کليدي: سيستم برنامه‌ريزي منابع سازماني، امنيت اطلاعات، امنيت متمرکز[3]، امنيت غيرمتمرکز[4]، مالکيت اطلاعات.

---

[1] Enterprise Resource Planning

[2] Information Ownership

[3] Centralized Security

[4] Decentralized Security

۱- مقدمه

استفادهٔ گسترده از سیستم‌هاي ERP در مقیاس بزرگ، موجب مي‌شود کاربران نهائي به اطلاعات حیاتي سازمان دسترسي داشته باشند. سازمان‌هایي که از این سیستم‌ها استفاده مي‌کنند، معمولاً اندازهٔ متوسط تا بزرگ دارند. چنین سازمان‌هایي نیاز به دسترسي به تمامي اطلاعات حوزهٔ کسب و کار دارند. در هر زمان، اطلاعات باید به‌صورت برخط در دسترس باشد تا سازمان بتواند واکنش‌هاي به‌موقعي را هنگام تغییر شرایط از خود بروز دهد. بسته به سطح یکپارچگي، دسترسي به سیستم ERP ممکن است از سطح کارگران تا مدیر اصلي سازمان، توسعه داشته باشد. سطح بالاي یکپارچگي، موجب به‌وجود آمدن مسائل امنیتي متعددي مي‌شود. باید توجه داشت که حفاظت از دارایي‌ها و اطلاعات سازمان، از مهمترین اصول است و براي حفاظت از این دارایي‌ها باید به مقولهٔ امنیت توجه خاص داشت.

ساز و کارهاي گوناگوني به‌منظور تأمین امنیت، توسط ERPهاي موجود، ارائه شده است. ساز و کار اولیهٔ پشتیباني شده به‌وسیلهٔ این سیستم‌ها، کنترل دسترسي و تصدیق هویت کاربر است[۱]. در حال حاضر، بحث امنیت بر اساس احراز هویت کاربر و دادن مجوزهایي به آن یا از طریق تعیین نقش و پروفایل است و انجام این موارد نیز به‌صورت متمرکز و از طریق گروه مدیریت امنیت اطلاعات انجام مي‌شود. این شیوهٔ مدیریت امنیت داراي مشکلات و معضلاتي است که از جملهٔ مهمترین آنها مي‌توان مورد ذیل را نام برد:

لازم است کلیهٔ اعضا گروه مدیریت امنیت اطلاعات به تمامي فرآیندهاي کسب و کار، اطلاعات، وظائف کارمندان و سطوح دسترسي مجاز، آشنایي کامل داشته باشند.

واضح است که تشکیل چنین تیمي بسیار دشوار بوده و از لحاظ امنیتي نیز داراي ایراداتي است.

لازم به ذکر است که با توجه به سابقه و قدمت سیستم‌هاي ERP و نیز بررسي‌هاي به‌عمل آمده، بحث امنیت سیستم‌هاي ERP، یك بحث نو بوده و تاکنون کارهاي زیادي در این مقوله انجام نشده است. طي تحقیقات انجام شده، از جمله فعالیت‌هایي که در این زمینه تاکنون صورت پذیرفته است مي‌توان موارد ذیل را نام برد:

- موضوع امنیت در ERPهاي موجود، مد نظر قرار گرفته است ولي چگونگي طراحي و پیاده‌سازي آن در یك ERP با ERP دیگر متفاوت است[۲].
- چك لیست‌هایي درخصوص امنیت سیستم‌هاي ERP تهیه شده است که این چك لیست‌ها فقط مي‌توانند در فاز انتخاب ERP، یاري‌دهندهٔ سازمان باشند[۳].
- چك لیست‌هایي جهت بررسي و کنترل امنیت اطلاعات در سیستم‌هاي ERP، تهیه شده است که این چك لیست‌ها جهت کنترل وضعیت امنیت در سیستم‌هاي ERP، مورد استفاده قرار مي‌گیرند[۳].
- چارچوبي بمنظور تجزیه و تحلیل تهدیدهاي امنیتي سیستم‌هاي ERP ارائه شده است[٤].

- رويكردي بالا به پايين[1] كه رويكردي جديد در مديريت ريسك سيستم‌هاي ERP است، ارائه شده است[٥].
- مدلي براي پيش‌بيني آسيب‌پذيري ارائه شده است[٦].
- تجزيه و تحليلي براي مخاطرات آسيب‌پذيري رايانه‌اي ارائه شده است[٧].
- يك چارچوب امنيتي براي يك سيستم ERP ارائه شده است[٨].

در حال حاضر، شركت‌هاي بزرگي در كشور ما در مراحل مختلف پياده‌سازي و استفاده از سيستم‌هاي ERP هستند كه از جملة مهمترين آنها مي‌توان شركت‌هاي ذيل را نام برد:

- ايران خودرو (با محصول SAP) [٩].
- ذوب آهن اصفهان (با محصول Oracle E-Business Suite) [١٠] و [١١].
- شركت ملي صنايع مس ايران (با محصول Ellipse) [١٢].
- مديريت برق آذربايجان (با محصول IFS) [١٣].
- گل گهر سيرجان (با محصول Oracle E-Business Suite) [١٤].
- توگا-گروه مپنا (با محصول SAP) [١٥].

همچنين تعداد بسيار زيادي از شركت‌هاي ديگر تصميم به استفاده و پياده‌سازي سيستم‌هاي ERP گرفته‌اند كه روز به روز بر تعداد اين شركت‌ها افزوده مي‌شود. از سوي ديگر، شركت‌هاي داخلي زيادي درصدد ايجاد و ارائة اين سيستم‌ها هستند كه برخي نيز محصولاتي ارائه و در برخي شركت‌ها پياده‌سازي كرده‌اند كه در اينجا از ذكر نام اين شركت‌هاي داخلي صرف نظر مي‌شود.

با توجه به شرايط خاص كشور، بحث امنيت اطلاعات مورد توجه خاص دولتمردان ومسئولين كشورمان قرار گرفته است به‌نحوي كه هر روز شاهد ارائة سمينارها، دستورالعمل‌ها و بخشنامه‌هايي در اين زمينه بوده و سازمان‌ها و شركت‌ها نيز توجه خاصي به اين مقوله دارند.

با عنايت به موارد ذكر شدة فوق و درنظر گرفتن شرايط خاص ايران و همچنين مسائل فرهنگي اجتماعي، توجه خاص به اين مسائل مي‌تواند كمك بسزائي در حفظ امنيت اطلاعات شركت‌هاي استفاده كننده از سيستم‌هاي ERP و نيز راه‌گشائي براي شركت‌هاي ارائه‌كنندة اين سيستم‌ها و به‌خصوص شركت‌هاي داخلي باشد.

هدف از ارائة اين مقاله، بررسي زيرسيستم امنيت در سيستم‌هاي ERP مطرح فعلي و شناسائي نقاط ضعف، كاستي‌ها و مشكلات موجود در زيرسيستم امنيت اين سيستم‌ها است. همچنين يك طرح امنيتي ارائه خواهد شد كه با استفاده يا جايگزين كردن آن در زيرسيستم‌هاي امنيت فعلي، تا حدود زيادي مشكلات بيان شده، مرتفع خواهند شد.

ساختار ادامة اين مقاله به اين صورت است كه در بخش دوم، تعاريف و برخي مسائل مرتبط با سيستم‌هاي برنامه‌ريزي منابع

---

[1] Top-down Approach

سازماني بيان شده است. در بخش سوم، موضوع امنيت برخي سيستم‌هاي ERP مورد بررسي قرار گرفته است. در بخش چهارم، نتايج اين پژوهش كه ارائة يك طرح امنيتي است ارائه شده است و در خاتمه، در بخش پنجم، يك جمع‌بندي براي اين پژوهش و پيشنهادهاي مطالعاتي و تحقيقاتي بيان شده است.

۲- سيستم برنامه‌ريزي منابع سازماني

۱-۲ **ERP** چيست؟

براي سيستم‌هاي برنامه‌ريزي منابع سازماني تعاريف متعددي ارائه شده است ولي از آنجا كه تاكنون تعريفي به‌صورت استاندارد تعريف نشده است كه همگان بر آن اتفاق نظر داشته باشند، برخي از اين تعاريف در ذيل ارائه مي‌شوند:

- تعريف عاميانه: ERP، يك راه حل نرم‌افزاري است كه مي‌كوشد كلية فعاليت‌هاي واحدهاي مختلف سازمان را به‌طور يكپارچه در يك سيستم نرم‌افزاري واحد تعريف و ايجاد كند به‌نحوي‌كه آن واحدها بتوانند نيازهاي كاري و اطلاعاتي خود را از آن دريافت كنند.
- تعريف انجمن بين‌المللي داده (IDC)[1]: ERP، نرم‌افزار و سيستمي است كه فرآيندهاي كاري يك سازمان را با به‌كارگيري واسط كاربر يكپارچه، داده‌ها و بانك اطلاعاتي يكپارچه و زبان برنامه‌سازي يكپارچه مكانيزه مي‌كند.
- ERP، سيستم نرم‌افزاري براي مديريت كسب و كار است كه حوزه‌هاي عملياتي مانند برنامه‌ريزي، توليد، فروش، بازاريابي، توزيع، حسابداري، مالي، نيروي انساني، مديريت پروژه، مديريت موجودي، نگهداري و تعميرات، حمل و نقل و تجارت الكترونيكي را پشتيباني مي‌كند[۱٦].
- ERP، بستة نرم‌افزاري جامعي است كه اطلاعات و فرآيندهاي مبتني بر اطلاعات را در تمامي حوزه‌هاي عملياتي يك سازمان ادغام مي‌كند[۱۷].
- تعريف انجمن كنترل توليد و موجودي آمريكا (APICS)[2]: ERP، روشي است براي برنامه‌ريزي و كنترل مؤثر تمامي منابع مورد نياز براي دريافت، توليد، ارسال و پاسخگوئي به نيازهاي مشتريان در شركت‌هاي توليدي، توزيعي و خدماتي[۱۸].
- ERP، یک بستة نرم افزاري تجاري است كه هدف آن يكپارچگي اطلاعات و جريان اطلاعات بين تمامي بخش‌هاي سازمان از جمله مالي، حسابداري، منابع انساني، زنجيرة عرضه و مديريت مشتريان است[۱۸].
- سيستم‌هاي ERP، سيستم‌هاي اطلاعاتي قابل تغيير و تنظيمي هستند كه اطلاعات و فرآيندهاي مبتني بر اطلاعات سازمان را درون واحدهاي سازماني و بين آنها، يكپارچه مي‌كنند[۱۸].
- ERP، يك پايگاه داده، يك برنامة كاربردي و يك واسط يكپارچه در تمامي سازمان است[۱۸].

---

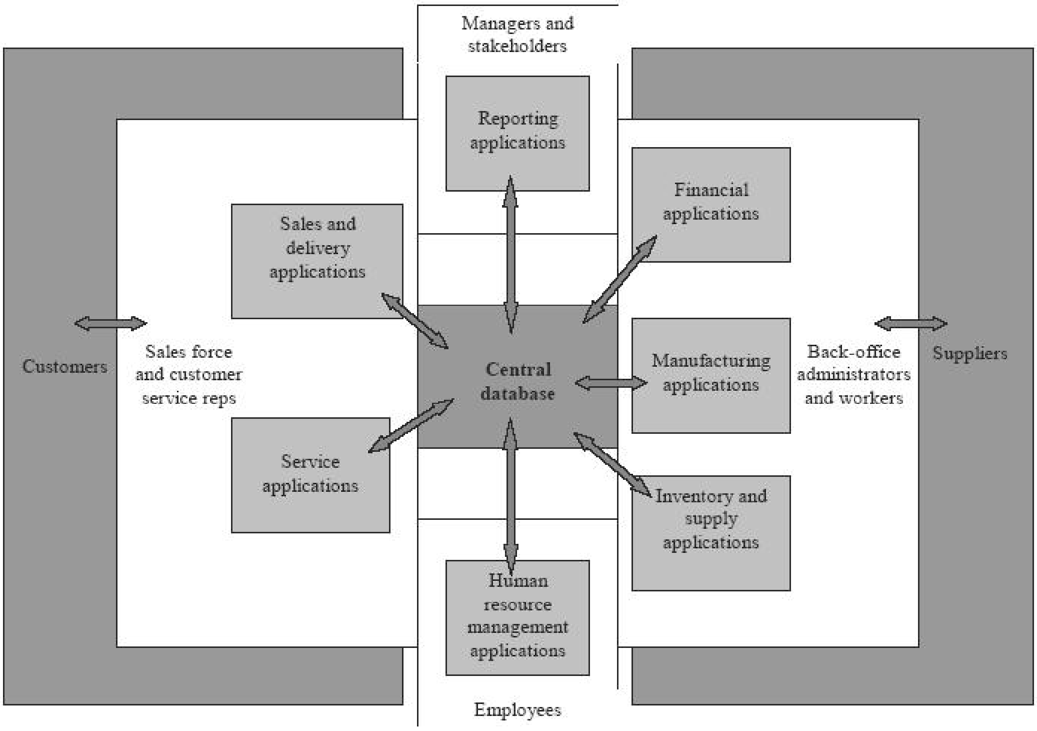
[1] International Data Corporation

[2] American Production Inventory Control Society

- ERP، سيستم‌هاي مبتني بر رايانه هستند كه براي پردازش تراكنش‌هاي سازمان طراحي شده‌اند و هدف آنها تسهيل برنامه‌ريزي، توليد و پاسخگوئي به‌موقع به مشتريان در محيطي يكپارچه است[۱۸].
- ERP، يك بستة نرم‌افزاري استاندارد مشتمل بر چندين ماژول مرتبط و يكپارچه است كه كلية فرآيندهاي تجاري يك سازمان را اعم از توليد، منابع انساني، مالي، بازاريابي و فروش پشتيباني مي‌كند و منجر به يكپارچگي وظائف در سازمان مي‌شود[۱۸].
- ERP، يك راه‌حل سيستمي مبتني بر فناوري اطلاعات است كه منابع سازمان را توسط يك سيستم به‌هم‌پيوسته، به سرعت و با دقت و كيفيت بالا، در كنترل مديران سطوح مختلف سازمان قرار مي‌دهد تا به‌طور مناسب فرآيند برنامه‌ريزي و عمليات سازمان را مديريت كنند[۱۸].
- ERP، به مثابه ستون فقرات اطلاعاتي يك سازمان از لحاظ بانك‌هاي اطلاعاتي وفرآيندهاي سازماني محسوب شده و به منزلة نرم‌افزاري براي پشتيباني فرآيندهاي داخلي سازمان است[۱۸].
- ERP، محصولي است كه از طريق به‌كارگيري يك واسط كاربر يكپارچه، يك مجموعة دادة يكپارچه و يك مجموعه كد يكپارچه، به خودكارسازي فرآيندهاي كسب و كار يك سازمان كمك مي‌كند[۱۹].
- ERP، يك سيستم اطلاعاتي است كه تمامي منابع موجود در يك سازمان را مديريت مي‌كند[۱۹].

ساختار كلان يك سيستم ERP در شكل ۲-۱ نشان داده شده است[۲۰].

ofSID


Managers and stakeholders
Reporting applications
Sales and delivery applications
Financial applications
Customers
Sales force and customer service reps
Central database
Manufacturing applications
Back-office administrators and workers
Suppliers
Service applications
Inventory and supply applications
Human resource management applications
Employees

شكل (۲-۱) ساختار كلان سيستم **ERP**

۲-۲ عدم موفقيت برخي پروژه‌هاي **ERP**

به زبان ساده، ERP مجموعة نرم‌افزاري است كه برگرفته از استانداردها و تجربيات موفقي است كه براي كمك به بهبود انجام فعاليت‌هاي مالي، توليدي، بازرگاني و پشتيباني در سازمان بكار گرفته مي‌شوند. براي اخذ بهترين نتايج، سازمان بايستي از كاركنان خود بخواهد روش‌هاي كاري خود را با سيستم جديد تطبيق دهند. اگر كاركنان بخش‌هاي مختلف احساس نكنند كه روش كاري ارائه شده در سيستم جديد بهتر از روش قديمي است كه آنها به آن عادت دارند، مقاومت كرده و يا خواهند خواست كه نرم افزار مطابق خواستة آنها تغيير كرده يا به اصطلاح Customize شود. در اينجاست كه پروژة ERP با بحران مواجه خواهد شد؛ كشمكش‌ها شروع شده و پروژه در باتلاق طولاني و پرهزينة Customization، براي نيل به خواسته‌هاي افراد قدرتمند قسمت‌هاي مختلف فرو خواهد رفت. تغيير زياد، نرم افزار را ناپايدار كرده و نگهداري، پشتيباني و بروزرساني آنرا سخت مي‌كند. بررسي داستان‌هاي غم‌انگيز عدم موفقيت برخي از پروژه‌هايERP، نشان داده است كه علت اصلي آن، تغييرات زيادي بوده كه سازمان‌ها براي تطبيق روش‌هاي كاري قديمي خود در هستة نرم‌افزار ERP داده‌اند[۲۱]. جدا از اين مسائل، عوامل مديريتي ذيل تأثير بسزائي در عدم موفقيت هر پروژه‌اي و به‌طور خاص پروژه‌هايERP دارد:

- برنامه‌ريزي و طراحي ناكافي.
- مقاومت در برابر تغيير.
- عدم ضمانت كافي.
- مديريت ضعيف پروژه.
- مديريت تغيير[۱] ضعيف.
- عدم تبيين دقيق انتظارات از سيستم.
- تغيير شرايط داخلي و خارجي.
- مشكلات ناشي از مشاور.
- نقائص و مشكلات مربوط به امنيت سيستم.

۳- مشكلات امنيتي برخي سيستم‌هاي **ERP** موجود

۱-۳ **Oracle E-Business Suite**

اين محصول، مسائل مربوط به امنيت را در داخل خود حل و فصل مي‌كند. اين برنامه، كلية كارهاي مربوط به تصديق هويت را انجام مي‌دهد. جزئيات مربوط به نقش‌ها و مسئوليت‌هاي كاربراني كه وارد سيستم مي‌شوند در جداول بانك اطلاعاتي

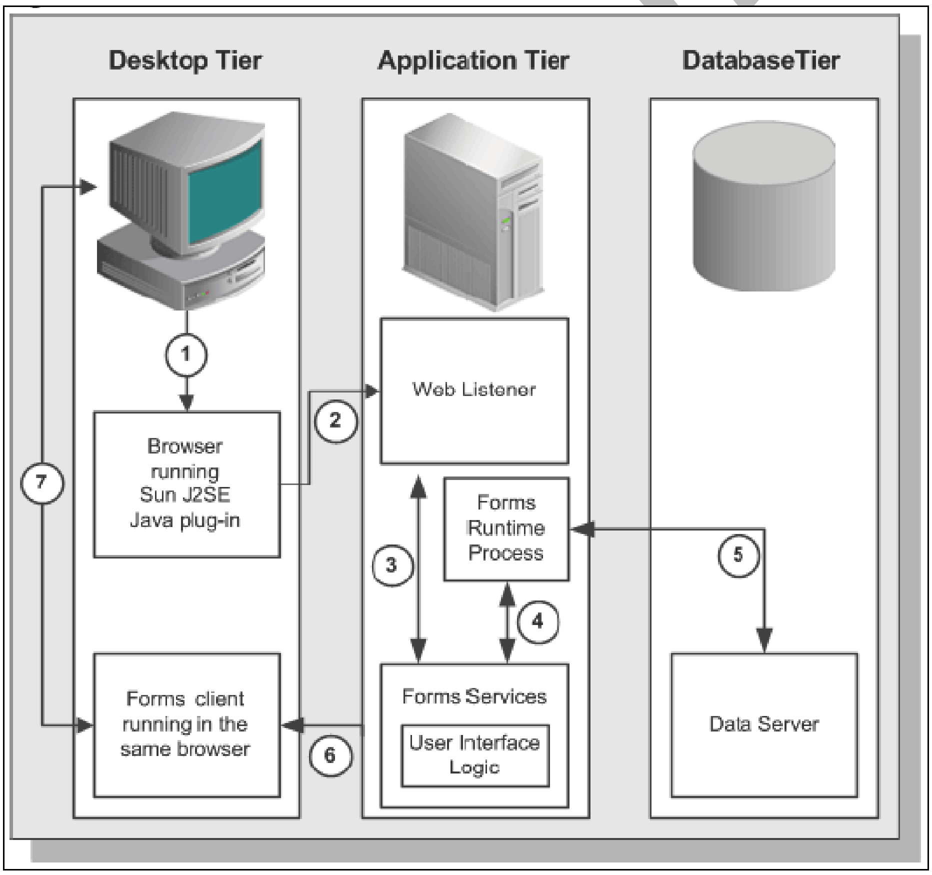
---

[1] **Change Management**

نگهداري مي‌شوند. پس از ورود كاربر به سيستم، يك منو از گزينه‌هايي نمايش داده مي‌شود كه مجاز به اجراي آنها است. اين منوهاي كاربر، توسط مدير فني سيستم و در زماني‌كه سطوح دسترسي تعريف مي‌شوند ايجاد مي‌شوند.

Oracle E-Business Suite، تعدادي نقش و مسئوليت ازپيش‌تعريف‌شده كه مي‌توانند به كاربران تخصيص يابند، در اختيار مي‌گذارد. هر نقش مي‌تواند شامل چندين مسئوليت باشد. يك مسئوليت، به يك عمل منفرد كه ممكن است كاربر انجام دهد اطلاق مي‌شود؛ مانند خريد و يا ارسال يك سند مالي. نقش‌ها به پرونده‌هاي اطلاعاتي كاربران[1] نسبت داده مي‌شوند.

پس از اتصال كاربر به سيستم، يك سرويس دهندة وب[2]، نام كاربري و كلمة عبور را كنترل مي‌كند. درصورت صحت اعتبار كاربر، يك سطر نشست[3] در بانك اطلاعاتي ايجاد مي‌شود. اين سطر نشست، يك شماره به مرورگر وب كاربر برمي‌گرداند. اين شماره به‌منظور كنترل صحت درخواست‌هاي اوليه كه از سوي كاربر براي برنامه ارسال مي‌شود، مورد استفاده قرار مي‌گيرد. اين عمليات در شكل ۳-۱ نشان داده شده است[۲۲].


Desktop Tier
Application Tier
DatabaseTier
1
Browser running Sun J2SE Java plug-in
2
Web Listener
3
Forms Runtime Process
4
5
Forms client running in the same browser
6
Forms Services
User Interface Logic
7
Data Server

شكل (۳-۱) نحوة برقراري ارتباط كاربر با **Oracle E-Business Suite**

---

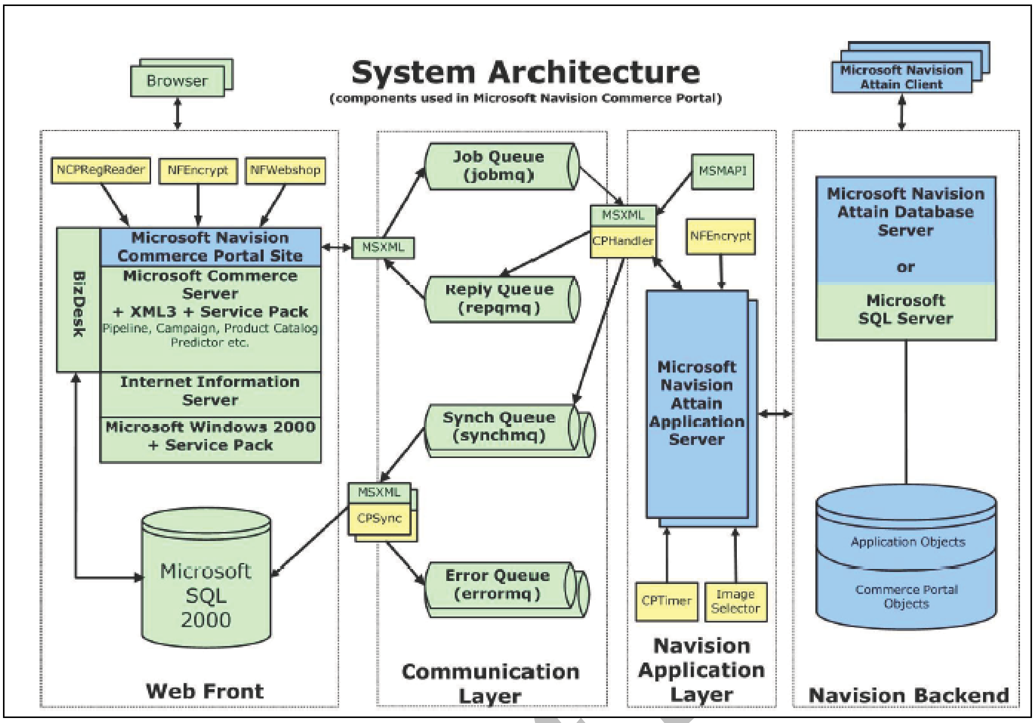
1 User Master Record
2 Web Server
3 Session Row

نقاط ضعف امنيتي موجود در Oracle E-Business Suite، در دو گروه خاص محصول و مشترك، به‌شرح ذيل است:

- نقاط ضعف خاص محصول:
  - امنيت اشيا تغييريافته، مسئله‌ساز است. برنامه‌نويسان اين‌گونه اشيا بايد كنترل امنيت مربوطه را در كد خود اضافه كنند. كارآيي اين روش براي ردگيري و مميزي، دشوار است.
  - روال كنترل امنيت، ساده و كلي بوده و برخي نيازها را پوشش نمي‌دهد.
  - نقش‌هاي استاندارد ارائه شده، بسيار كلي هستند؛ به‌گونه‌اي كه نمي‌توان براي هر موردي، از آنها استفاده كرد.
  - مديريت پروندة اطلاعاتي كاربر، هيچ‌گونه تسهيلاتي جهت معاوضة نقش كاربران ارائه نمي‌كند. اين مورد هنگامي اهميت پيدا مي‌كند كه كاربري قادر به كار با سيستم نباشد و كاربر ديگري بايد وظيفة وي را انجام دهد.
- نقاط ضعف مشترك:
  - رويكردي كاملاً متمركز در پياده‌سازي امنيت.
  - عدم پشتيباني از مفهوم مالكيت اطلاعات.
  - پشتيباني ضعيف از تعيين و كنترل تفكيك وظائف. اين مورد، نتيجة مستقيم فقدان مالكيت اطلاعات است.
  - سختي كنترل دسترسي در تمامي ماژول‌ها يا نواحي كاري درون سيستم.
  - فقدان يك متدولوژي رسمي براي پياده‌سازي زيرسيستم امنيت.
  - نياز به مهارت‌هاي بالاي فني براي طراحي و پياده‌سازي زيرسيستم امنيت.
  - پشتيباني كم نرم‌افزار از مستندسازي كه موجب ردگيري دشوار و زمان‌بر مي‌شود.
  - فقدان مديريت تغيير براي تمام اشيا امنيتي كه موجب ردگيري دشوار و بررسي بسيار مشكل تغييرات مي‌شود.

٢-٣ Microsoft Navision Attain

اين محصول از يك بانك اطلاعاتي رابطه‌اي مخصوص به خود استفاده مي‌كند؛ اگرچه، سيستم مديريت بانك اطلاعاتي Microsoft SQL Server نيز پشتيباني مي‌شود. بانك اطلاعاتي Microsoft Navision Attain به‌علت سهولت نگهداري، هزينة كمتري را به سازمان تحميل مي‌كند. Microsoft SQL Server نيز براي سازمان‌هاي بزرگ پيشنهاد مي‌شود.Microsoft Navision Attain بر روي سيستم‌هاي عامل Microsoft Windows اجرا مي‌شود و كاربران از طريق يك نرم‌افزار نهائي كه بر روي ايستگاه كاري آنها نصب مي‌شود، به سيستم متصل مي‌شوند. نمايي كلي از معماري Microsoft Navision Attain در شكل ٣-٢ نشان داده شده است[٢٣].


System Architecture
(components used in Microsoft Navision Commerce Portal)
Browser
Microsoft Navision Attain Client
NCPRegReader
NFEncrypt
NFWebshop
BizDesk
Microsoft Navision Commerce Portal Site
Microsoft Commerce Server
+ XML3 + Service Pack
Pipeline, Campaign, Product Catalog Predictor etc.
Internet Information Server
Microsoft Windows 2000 + Service Pack
Microsoft SQL 2000
Web Front
MSXML
Job Queue (jobmq)
Reply Queue (repqmq)
Synch Queue (synchmq)
MSXML
CPSync
Error Queue (errormq)
Communication Layer
MSXML
CPHandler
MSMAPI
NFEncrypt
Microsoft Navision Attain Application Server
CPTimer
Image Selector
Navision Application Layer
Microsoft Navision Attain Database Server
or
Microsoft SQL Server
Application Objects
Commerce Portal Objects
Navision Backend

شكل (٣-٢) نمايي كلي از معماري **Microsoft Navision Attain**

Navision Attain داراي يك زيرسيستم امنيت داخلي است. پياده‌سازي اين سيستم امنيت، توسط مدير امنيت و به كمك اشيائي كه در بانك اطلاعاتي ذخيره مي‌شوند انجام مي‌شود. مدير امنيت، عمليات مجاز بر روي اين اشيا را براي هر كاربر انتخاب مي‌كند. اين تنظيمات، براي هر كاربر به‌صورت نقش، ذخيره مي‌شود. تعدادي نقش از پيش تعريف شده، هنگام نصب نرم‌افزار ارائه مي‌شود ولي امكان ايجاد نقش‌هاي اضافي نيز وجود دارد.

از آنجاكه سطوح زيادي در تنظيمات امنيتي تعريف نشده است، سازمان‌هاي مختلف ممكن است وضعيت موجود را تغيير داده يا نقش‌ها و اشيا جديدي ايجاد كنند.

نقاط ضعف امنيتي موجود در Microsoft Navision Attain ، در دو گروه خاص محصول و مشترك، بشرح ذيل است:

- نقاط ضعف خاص محصول:
  - محافظت اشيا توسعه و يا تغييريافته، مسئله‌اي دشوار و پيچيده است. برنامه‌نويسان اشيا سفارشي بايد كنترل‌هاي مربوط به امنيت را در كد خود ايجاد كنند. كارآيي اين كنترل‌ها در رديگري و بازبيني پايين است.
  - روال كنترل امنيت، ساده و كلي بوده و برخي نيازها را پوشش نمي‌دهد.
  - در اين سيستم، نقش‌ها وجود دارند ولي مديريت امنيت مجبور نيست از يك رويكرد كاملاً نقش-محور به‌منظور اعمال امنيت استفاده كند.

  - نقش‌هاي استاندارد ارائه شده توسط اين سيستم، بسيار كلي هستند به‌نحوي‌كه نمي‌توان براي هر كاربردي از آنها استفاده كرد.
  - مديريت پروندة اطلاعاتي كاربر، روشي ساده براي تغيير نقش‌ها از يك كاربر به كاربر ديگر در اختيار نمي‌گذارد. اين مورد هنگامي اهميت پيدا مي‌كند كه يك كاربر، قادر به كار با سيستم نباشد.
- نقاط ضعف مشترك:
  - يك رويكرد كاملاً متمركز براي پياده‌سازي امنيت.
  - عدم پشتيباني از مفهوم مالكيت اطلاعات.
  - پشتيباني ضعيف براي تعيين و كنترل تفكيك وظائف.
  - سختي در انجام كنترل دسترسي به ماژول‌هاي مختلف يا نواحي كاري نرم‌افزار.
  - فقدان يك متدولوژي پياده‌سازي جامع و رسمي مربوط به زيرسيستم امنيت.
  - نياز به دانش فني بالا براي طراحي و پياده‌سازي زيرسيستم امنيت.
  - مستندسازي كم توسط نرم‌افزار كه موجب طولاني و مشكل شدن عمليات مربوط به ردگيري و مميزي مي‌شود.
  - فقدان مديريت تغيير براي تمام اشيا امنيتي كه موجب مي‌شود ردگيري و بررسي تغييرات، بسيار مشكل شود.

۳-۳ SAP/R3

سيستم SAP، قابليت امنيت را به‌صورت داخلي فراهم مي‌كند كه معمولاً به آن، مفهوم مجوزدهي SAP اطلاق مي‌شود. پياده‌سازي اين مفهوم مجوزدهي، از طريق تعدادي جدول بانك اطلاعاتي كه شامل اطلاعات مرتبط با امنيت هستند محقق مي‌شود. به‌منظور كنترل اينكه آيا يك كاربر خاص، مجوز اجراي يك تابع معين يا دستكاري اطلاعات به‌خصوصي را دارد، مراجعات زيادي به اين جداول مورد نياز است. وابسته به محتويات اين جداول، مجوز دسترسي به تابع يا اطلاعات، صادر يا سلب مي‌شود.

نوع امنيت پياده‌سازي شده با استفاده از مدل مجوزدهي SAP، ممكن است وابسته به سازماني باشد كه از سيستم SAP استفاده مي‌كند. به‌عنوان مثال، ممكن است سازمان‌هاي بزرگ نيازهاي سخت‌گيرانه‌تري نسبت به سازمان‌هاي كوچك داشته باشند. در ادامه، نقاط ضعف موجود در اين محصول، در دو گروه: مشكلات خاص محصول و مشكلات مشترك آمده است.

- نقاط ضعف خاص محصول:
  - امنيت اشيا تعريف شده توسط مشتري، مشكل آفرين است. ايجاد كنندگان اين اشيا بايد كنترل‌هاي امنيتي را در كد برنامة خود ايجاد كنند. مميزي و بررسي اين تغييرات بسيار مشكل و كارآيي آن پايين است.

  - روال كنترل امنيت، ساده و كلي است و برخي نيازها را پوشش نمي‌دهد.
  - امكان استفاده از نقش وجود دارد ولي مديريت امنيت، ملزم به استفاده از رويكرد نقش-محور امنيت نيست.
  - نقش‌هاي استاندارد ارائه شده توسط SAP بسيار كلي هستند به‌نحوي‌كه نمي‌توان براي هر كاربردي از آنها استفاده كرد و براي نيازهاي سازمان مشتريان، مناسب نيستند. استفاده از اين‌گونه نقش‌هاي استاندارد، ممكن است با امنيت سيستم در تضاد باشد.
  - كنترل دسترسي كاربر به گزارش‌ها و اجراي برنامه‌ها مشكل است مگر اينكه كدهاي مجوز خاصي براي اين اشيا اضافه شود. در بسياري حالات، دسترسي به برنامه‌ها و گزارش‌ها، بدون واگذاري مقادير خاص دسترسي به كاربر، امكان‌پذير است.
  - مديريت پروندة اطلاعاتي كاربر، روش ساده‌اي براي انتساب نقش‌هاي يك كاربر به كاربر ديگر ارائه نمي‌كند.

- نقاط ضعف مشترك محصول:
  - يك رويكرد كاملاً متمركز براي پياده‌سازي امنيت.
  - فاقد هرگونه امكان براي پشتيباني مفهوم مالكيت اطلاعات.
  - پشتيباني ضعيف تعيين و كنترل تفكيك وظائف.
  - دشواري كنترل دسترسي در ماژول‌هاي مختلف يا نواحي كاري نرم‌افزار.
  - فقدان يك متدولوژي پياده‌سازي جامع و رسمي زيرسيستم امنيت.
  - نياز به مهارت‌هاي فني سطح بالا براي طراحي و پياده‌سازي زيرسيستم امنيت.
  - مستندسازي ناچيز نرم‌افزار و در نتيجه، رديابي زمانبر و مشكل.
  - فقدان مديريت تغيير براي تمامي اشيا امنيت و درنتيجه، بررسي و كنترل بسيار سخت تغييرات.

۳-٤ جمع‌بندي

در بخش‌هاي گذشته، برخي از مشكلاتي كه در حوزة امنيت اكثر سيستم‌هاي ERP وجود دارند، ارائه شد. ‌به‌طور خلاصه مي‌توان موارد مشترك مطرح شده را به‌صورت ذيل بيان كرد:

- پياده‌سازي امنيت سيستم‌هاي ERP، بصورت متمركز انجام مي‌شود.
- نتيجة رويكرد متمركز پياده‌سازي امنيت در سيستم‌هاي ERP اين است كه مفهوم مالكيت اطلاعات به فراموشي سپرده مي‌شود.
- عدم پشتيباني از مفهوم مالكيت اطلاعات موجب مي‌شود در تفكيك وظائف ممكن، كمكي به سازمان نشود.

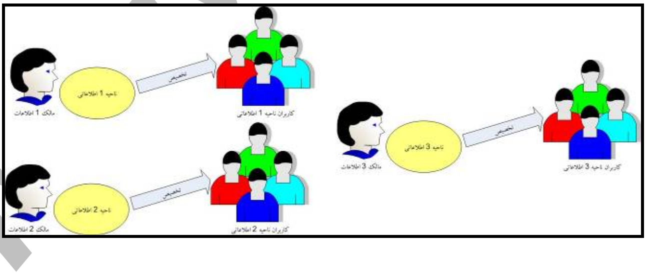
- بدون داشتن دسترسي به يك روش آسان تفكيك وظائف، ممكن است مخاطراتي سازمان را تهديد كند.
- پشتيباني ضعيف از موارد مربوط به نظارت سازماني، به‌خصوص مواردي كه توسط قانون وضع مي‌شوند، در سيستم‌هاي ERP مشهود است.
- هيچيك از سيستم‌هاي ERP شناسايي شده، متدولوژي جامع و كاملي براي پياده‌سازي امنيت ارائه نمي‌كنند.
- پياده‌سازي امنيت، به‌جاي تمركز بر موضوعات كسب و كار، بر جنبه‌هاي فني تأكيد دارد.
- سيستم‌هاي ERP بررسي شده، مستندسازي كمي درخصوص اشيا امنيتي ارائه مي‌كنند.

و در انتها بايد اشاره كرد كه مالكيت اطلاعات و مديريت مخاطرات، مهمترين مفاهيمي هستند كه مي‌توانند در بهبود امنيت سيستم‌هاي ERP مورد توجه قرار گيرند.

٤- طرح پيشنهادي

٤-١ مفهوم مالكيت اطلاعات

مفهوم مالكيت اطلاعات، هستة مركزي طرح پيشنهادي را شكل مي‌دهد و بدين معنا است كه افرادي مجزا، مسئول نواحي مشخصي از كسب و كار هستند. اين افراد، مالكان اطلاعات ناميده مي‌شوند. مالكان اطلاعات قادر هستند دسترسي كاربران را به سيستم به‌منظور اجراي توابع مشخص تعريف كنند. مسئوليت كامل تخصيص مجوزهاي سيستم، بر عهدة مالكان اطلاعات است. يك مدل سطح خيلي كلان اين پروسه، در شكل ٤-١ آمده است.


مالک 1 اطلاعات
ناحیه 1 اطلاعاتی
تخصیص
کاربران ناحیه 1 اطلاعاتی
مالک 2 اطلاعات
ناحیه 2 اطلاعاتی
تخصیص
کاربران ناحیه 2 اطلاعاتی
مالک 3 اطلاعات
ناحیه 3 اطلاعاتی
تخصیص
کاربران ناحیه 3 اطلاعاتی

شكل (٤-١) مالكيت اطلاعات در معماري پيشنهادي

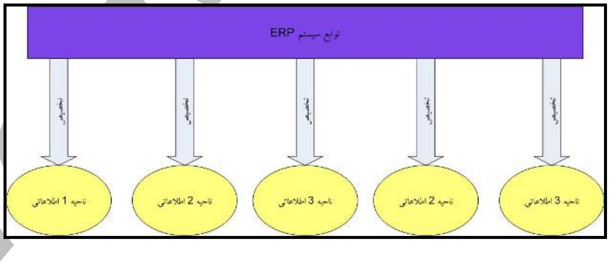
شكل ٤-١، مالكيت يك حوزة اطلاعاتي را براي يك مالك اطلاعات نشان مي‌دهد. حوزة اطلاعاتي كه به مالك اطلاعات تخصيص يافته، شامل تمامي توابع مربوط به يك ناحية خاصي از كسب و كار است. به‌خاطر وجود مفهوم مالكيت اطلاعات، مالكان اطلاعات، پاسخگوي سوء استفاده از سيستم ERP هستند.

٤-٢ مفهوم نواحي اطلاعاتي

مالكيت اطلاعات، به‌واسطة تقسيم توابع ارائه شده توسط سيستم ERP به گروه‌هاي مجزا، حاصل مي‌شود. اين گروه‌ها شامل توابعي هستند كه معمولاً به‌نحوي با يكديگر ارتباط دارند؛ به‌عنوان مثال تمام توابع مربوط به حقوق منابع انساني و يا سفارش كالا. تعيين اينكه كدام توابع بايد به چه ناحيه‌هايي تخصيص يابند، بر عهدة سازمان است. مي‌توان پيشنهادها و يا نمونه‌هايي را ارائه كرد ولي الزامي براي آنها وجود ندارد. نواحي اطلاعاتي به سازمان اجازه مي‌دهند تا بصورت يك مدل منطقي، تقسيم‌بندي شود. هدف از اين كار، افزايش كنترل به‌وسيلة تخصيص مسئوليت‌ها به هر ناحية مجزا است. مالكان اطلاعاتي، مسئول تخصيص مجوزهاي دسترسي به كاربران معمولي هستند.

سازمان مختار است نواحي اطلاعاتي را به‌گونه‌اي انتخاب كند كه بيشترين تناسب را با شرايط سازمان داشته باشند. ساده‌ترين شكل تقسيم‌بندي يك سازمان به نواحي اطلاعاتي، با استفاده از نواحي تابعي سيستم ERP انجام مي‌شود. به‌عنوان نمونه‌هايي از اين نواحي تابعي مي‌توان از مديريت مواد، مالي، فروش و منابع انساني نام برد. همچنين سازمان‌ها مجاز به انتخاب نواحي اطلاعاتي ديگري نيز هستند. سازمان‌هاي بزرگ و چند مليتي كه به‌صورت تخصصي در حوزه‌هاي مختلف تجاري فعاليت مي‌كنند، مي‌توانند طبقه‌بندي متفاوتي براي نواحي اطلاعاتي خود داشته باشند. به‌عنوان مثال، شركت بزرگي كه داراي بخش‌هاي نقليه، الكترونيك، پزشكي و فضائي است مي‌تواند همين بخش‌ها را به عنوان نواحي اطلاعاتي خود در نظر بگيرد ولي در عمل، سازمان مورد بحث، تصميم‌گيرندة نهايي درخصوص تعيين نواحي اطلاعاتي است.

شكل ٤-٢، فرآيند تخصيص توابع سيستم ERP را به نواحي مختلف اطلاعاتي نشان مي‌دهد.



شكل (٤-٢) نواحي اطلاعاتي

٤-٣ نقش‌ها

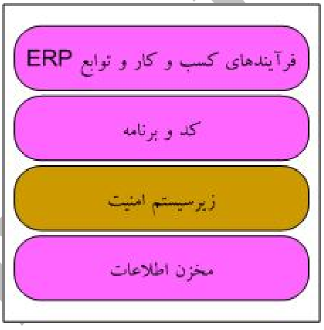
با بكارگيري يك سيستم ERP در سازمان، بايد بتوان تعيين كرد كه چه توابعي از سيستم ERP مورد استفاده قرار گيرند و براي برخي كاربران خاص، مجوز دسترسي به اين توابع صادر شود. معمولاً، در سيستم‌هاي ERP، اين عمل از طريق تعريف نقش‌ها و تخصيص آنها انجام مي‌شود. اين نقش‌ها شامل تمامي دسترسي‌هاي لازم به توابع مربوطه در سيستم هستند تا

اطمينان حاصل شود كه آن كاربران قادر به اجراي وظائفشان هستند.

در اين طرح، نقش‌ها در نواحي اطلاعاتي تعريف مي‌شوند. اين عمل توسط مالك اطلاعات انجام شده و نقش‌ها فقط به كاربراني تخصيص مي‌يابند كه به همان ناحية اطلاعاتي تعلق دارند. از اينرو، نقش‌ها نمي‌توانند فراتر از يك ناحية اطلاعاتي گسترش يابند. در عوض، درصورتي‌كه نياز باشد، يك كاربر مي‌تواند نقش‌هاي مختلفي را از نواحي اطلاعاتي مختلف اخذ كند. براي بيشتر كاربران، تخصيص يك نقش از يك ناحية اطلاعاتي كافي است.

٤-٤ جايگاه معماري

يك سيستم ERP، از تعداد بسيار زيادي مؤلفه تشكيل شده است. طرح پيشنهادي، يك طرح اوليه براي زيرسيستم امنيت يك سيستم ERP است. جايگاه زيرسيستم امنيت پيشنهادي، در شكل ٤-٣ نشان داده شده است. همانگونه كه مشاهده مي‌شود، اين زيرسيستم در لاية ٣ قرار گرفته است. ساير مؤلفه‌ها براي بيان موقعيت زيرسيستم امنيت، نمايش داده شده‌اند. مؤلفه‌هايي كه ذكر شده‌اند، براي پياده‌سازي معماري پيشنهادي، لازم و ضروري مي‌باشند.



شكل (٤-٣) جايگاه معماري پيشنهادي

تمركز اين مقاله بر روي لاية ٣ (زيرسيستم امنيت) خواهد بود. مخزن اطلاعاتي (لاية ٤) براي نگهداري كل داده‌هاي سيستم ERP، مورد نياز است. همانند كلية داده‌هاي سيستم ERP، اشيا و اطلاعات مرتبط با آنها كه توسط معماري پيشنهادي مديريت مي‌شوند، در لاية ٤ نگهداري مي‌شوند.

لاية كدنويسي (مؤلفة ٢) ايجاد و اجراي كد برنامه را فراهم مي‌كند. لاية كدنويسي شامل يك محيط برنامه‌نويسي براي برنامه‌نويسان و توسعه‌دهندگان و يك مفسر براي اجراي كد است. تمام توابع سيستم ERP در اين لايه قرار دارند. با اين وجود، تمامي كدها، در اشيا و جداول مخزن اطلاعاتي، ذخيره مي‌شوند.

كاركرد و تعامل سيستم ERP با كاربران، در لاية ١ نمايش داده مي‌شود. تلاش كاربران يا اشيا سيستم، براي دسترسي به توابع و اطلاعات محدود شده، در اين لايه صورت مي‌گيرد. زيرسيستم امنيت، صحت تمامي درخواست‌ها را تعيين مي‌كند.

٤-5 اجزا معماري

در جدول ٤-١، ساختار جداول اصلي كه جهت پياده‌سازي معماري پيشنهادي استفاده خواهند شد آمده است.

جدول (٤-١) ساختار جداول اصلي معماري

ErpInfoAreaTbl		نواحي اطلاعاتي
Field name	Type	Description
Name	STR	Name of information area
Description	STR	Description of information area
UserMasterRecordTbl		پروندة اطلاعاتي كاربر
UserName	STR	User name
Password	STR	Encrypted password
InfoAreaOwner	CHR	Indicates ownvership of an information area
SecurityAdmin	CHR	Indicates security administrator
InfoAreaID	NUM	Foreign key to ErpInfoAreaTbl
ValidStartDate	DAT	First date of validity
ValidEndDate	DAT	Last date of validity
PasswordExpirationAtFirstLogin	CHR	Indicates password should be expire at first login or not
StrongPasswordCheck	CHR	Indicates additional controls for password should be done or not
PasswordExpirationPeriod	NUM	Duration of password validity (in day)
PasswordExpirationConnCount	NUM	Valid number of login counts
ErpProgramTbl		برنامه‌ها
Name	STR	Name of program
CreateDate	DAT	Date of program creation
ChangeDate	DAT	Date of program modification
Type	STR	Type of program
Description	STR	Description of program
ErpFunctionTbl		توابع
FunctionCode	STR	Function code
ModuleID	NUM	Foreign key field to ErpInfoAreaTbl
ProgramID	NUM	Foreign key field to ErpProgramTbl
Description	STR	Description of module
ErpRoleTbl		نقش‌ها
Name	STR	Name of this role
Description	STR	Description of role
CheckObject	NUM	Foreign key field to ErpCheckObjectTbl
Action	NUM	Foreign key field to ErpActionTbl table

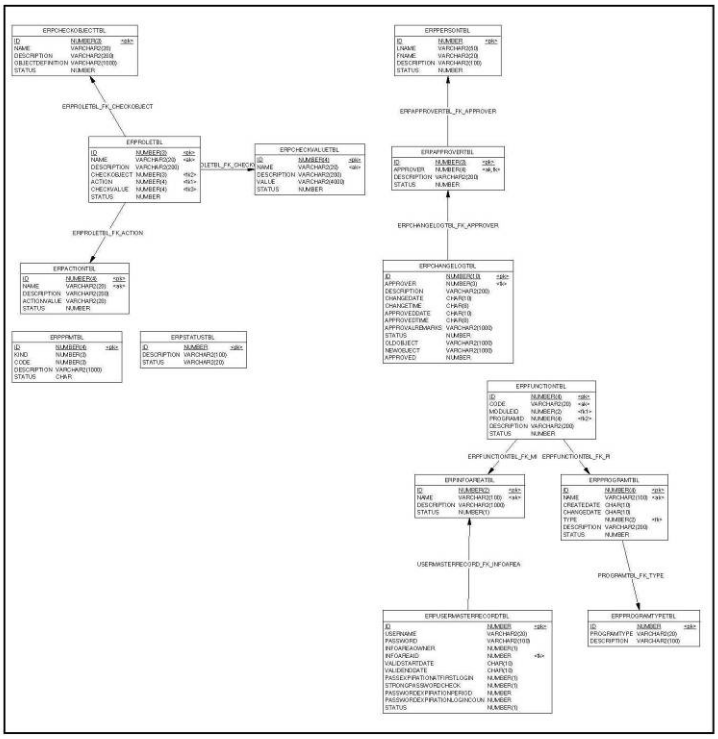
CheckValue	NUM	Foreign key field to ErpCheckValueTbl table
ErpCheckObjectTbl		اشيا كنترلي
Name	STR	Name of this check object
Description	STR	Check object description
ObjectDefinition	STR	Object definition for security object
ErpActionTbl		فعاليت‌ها
Name	STR	Name of this action
Description	STR	Action description
ActionValue	STR	Action-specific value
ErpCheckValueTbl		مقادير كنترلي
Name	STR	Name of this value
Description	STR	Value description
Value	STR	Value
ErpApproverTbl		تاييدكنندگان
Approver	NUM	Foreign key field to ErpUserMasterTbl table
Description	STR	Approver description
ErpChangeLogTbl		تغييرات
Approver	NUM	Foreign key field to ErpApproverTbl
Description	STR	Change description
Date	DAT	Date of change request registration
Time	TIM	Time of change request registration
ApprovedDate	DAT	Date of approval
ApprovedTime	TIM	Time of approval
ApprovalRemarks	STR	Some comments
OldObject	OBJ	Object prior to approval
NewObject	OBJ	Object after approval
Approved	CHR	Approval/Declined

تذكرات مهم:

١- در پياده‌سازي واقعي و بسته به نياز، فيلدهايي به اين جداول اضافه خواهند شد.

٢- در تمامي جداول، فيلدي با نام ID بمنظور كليد اصلي و فيلدي با نام Status بمنظور وضعيت ركورد جاري، در نظر گرفته خواهد شد كه در اينجا به‌منظور مختصر نويسي، از نمايش آنها صرف‌نظر شده است.

شكل ٤-٤، نمايي كلي از جداول معماري پيشنهادي را نشان مي‌دهد.


ERPCHECKOBJECTTBL
ID NUMBER(3) <pk>
NAME VARCHAR2(20)
DESCRIPTION VARCHAR2(200)
OBJECTDEFINITION VARCHAR2(1000)
STATUS NUMBER
ERPROLETBL_FK_CHECKOBJECT
ERPROLETBL
ID NUMBER(3) <pk>
NAME VARCHAR2(20) <ak>
DESCRIPTION VARCHAR2(200)
CHECKOBJECT NUMBER(3) <fk2>
ACTION NUMBER(4) <fk1>
CHECKVALUE NUMBER(4) <fk3>
STATUS NUMBER
OLETBL_FK_CHECK
ERPCHECKVALUETBL
ID NUMBER(4) <pk>
NAME VARCHAR2(20) <ak>
DESCRIPTION VARCHAR2(200)
VALUE VARCHAR2(4000)
STATUS NUMBER
ERPROLETBL_FK_ACTION
ERPACTIONTBL
ID NUMBER(4) <pk>
NAME VARCHAR2(20) <ak>
DESCRIPTION VARCHAR2(200)
ACTIONVALUE VARCHAR2(20)
STATUS NUMBER
ERPPRMTBL
ID NUMBER(4) <pk>
KIND NUMBER(3)
CODE NUMBER(3)
DESCRIPTION VARCHAR2(1000)
STATUS CHAR
ERPSTATUSTBL
ID NUMBER <pk>
DESCRIPTION VARCHAR2(100)
STATUS VARCHAR2(20)
ERPPERSONTBL
ID NUMBER <pk>
LNAME VARCHAR2(50)
FNAME VARCHAR2(20)
DESCRIPTION VARCHAR2(100)
STATUS NUMBER
ERPAPPROVERTBL_FK_APPROVER
ERPAPPROVERTBL
ID NUMBER(3) <pk>
APPROVER NUMBER(4) <ak,fk>
DESCRIPTION VARCHAR2(200)
STATUS NUMBER
ERPCHANGELOGTBL_FK_APPROVER
ERPCHANGELOGTBL
ID NUMBER(10) <pk>
APPROVER NUMBER(3) <fk>
DESCRIPTION VARCHAR2(200)
CHANGEDATE CHAR(10)
CHANGETIME CHAR(8)
APPROVEDDATE CHAR(10)
APPROVEDTIME CHAR(8)
APPROVALREMARKS VARCHAR2(1000)
STATUS NUMBER
OLDOBJECT VARCHAR2(1000)
NEWOBJECT VARCHAR2(1000)
APPROVED NUMBER
ERPFUNCTIONTBL
ID NUMBER(4) <pk>
CODE VARCHAR2(20) <ak>
MODULEID NUMBER(2) <fk1>
PROGRAMID NUMBER(4) <fk2>
DESCRIPTION VARCHAR2(200)
STATUS NUMBER
ERPFUNCTIONTBL_FK_MI
ERPFUNCTIONTBL_FK_R
ERPINFOAREATBL
ID NUMBER(2) <pk>
NAME VARCHAR2(100) <ak>
DESCRIPTION VARCHAR2(1000)
STATUS NUMBER(1)
ERPPROGRAMTBL
ID NUMBER(4) <pk>
NAME VARCHAR2(100) <ak>
CREATEDATE CHAR(10)
CHANGEDATE CHAR(10)
TYPE NUMBER(2) <fk>
DESCRIPTION VARCHAR2(200)
STATUS NUMBER
USERMASTERRECORD_FK_INFOAREA
PROGRAMTBL_FK_TYPE
ERPUSERMASTERRECORDTBL
ID NUMBER <pk>
USERNAME VARCHAR2(20)
PASSWORD VARCHAR2(100)
INFOAREAOWNER NUMBER(1)
INFOAREAID NUMBER <fk>
VALIDSTARTDATE CHAR(10)
VALIDENDDATE CHAR(10)
PASSEXPIRATIONATFIRSTLOGIN NUMBER(1)
STRONGPASSWORDCHECK NUMBER(1)
PASSWORDEXPIRATIONPERIOD NUMBER
PASSWORDEXPIRATIONLOGINCOUN NUMBER
STATUS NUMBER(1)
ERPPROGRAMTYPETBL
ID NUMBER <pk>
PROGRAMTYPE VARCHAR2(20)
DESCRIPTION VARCHAR2(100)

شكل (٤-٤) نمودار ارتباطي جداول معماري پيشنهادي

Archive of

۵- نتيجه‌گيري

به‌طور خلاصه، موارد و قابليت‌هايي كه با استفاده از اين معماري بدست خواهند آمد عبارتند از:

- پياده‌سازي واقعي امنيت نقش-محور.
- ايجاد مؤثر نقش‌ها.
- محدوديت دسترسي كاربران به گزارش‌ها و برنامه‌ها.
- مديريت مؤثر پروندة اطلاعاتي كاربران.
- پياده‌سازي امنيت غيرمتمركز.
- تفكيك وظائف.
- يكپارچگي ماژول‌ها.
- نظارت سازماني
- تمركز كمتر بر جنبه‌هاي فني.
- مستندسازي.

- مديريت تغيير.

طرح پيشنهاد شده در اين مقاله را بايد به‌عنوان اساس و پايه‌اي براي زيرسيستم بسته‌هاي نرم‌افزاري ERP آينده درنظر گرفت. به‌علت اينكه طرح پيشنهادي، به‌صورت كلي مطرح و تشريح شده است، كاربرد اين طرح بايد ارائه شده و در سيستم‌هاي ERP آتي مورد استفاده قرار گيرد. در مورد بسته‌هاي نرم‌افزاري ERP فعلي، كارهاي مجدد و تكراري قابل توجه و زيادي به‌منظور تطابق و يكپارچگي با اين طرح بايد انجام شوند. بايد توجه داشت كه ممكن است بسته‌هاي نرم‌افزاري ERP آينده، معماري مشابهي درخصوص زيرسيستم امنيت داشته باشند كه با مهمترين نيازها و كنترل‌هاي امنيتي مطابقت داشته باشند.

به‌طور خلاصه بايد گفت كه پياده‌سازي فني و واقعي اين معماري مي‌تواند به‌عنوان گام بعدي و فرصت مطالعاتي آتي درنظر گرفته شود. همچنين بايد توجه داشت كه اگرچه الحاق اين معماري به سيستم‌هاي ERP موجود، غيرممكن نيست ولي بسيار دشوار و پرهزينه است.

مراجع

[١] خندان. فرزاد، "امنيت در سيستم‌هاي برنامه‌ريزي منابع سازماني"، چهارمين همايش سالانة سيستم مديريت امنيت اطلاعات، مركز همايشهاي بين‌المللي صدا و سيما، تهران، ايران، آذر، ١٣٨۶.

[2] Marlene. Knigge, "Access Control in ERP Systems", Diploma Thesis, Univ. Hamburg, 22 December 2005

[3] Joy R. Hughes, Robert. Beer, "A Security Checklist for ERP Implementations", http://net.educause.edu/ir/library/pdf/EQM0741.pdf. (Visited on 2008-07-28).

[4] Roberta S. Russell, "A Framework for Analyzing ERP Security Threats", Department of Business Technology, Virginia Tech, Blacksburg, VA USA 2406l, http://www.cimap.vt.edu/CIIA/Papers/Session1-4-Russell.pdf. (Visited on 2008-07-05).

[5] D2C SOLUTIONS, "Thinking Top-Down: A New Approach to ERP Risk and Compliance Management", http://www.d2c.net/home/documents/WP_TopDown1.4.pdf. (Visited on 2008-06-21).

[6] Hein S. Venter, "A Model For Vulnerability Forcasting", Phd Thesis, Univ. Rand Afrikaans, May 2003

[7] Morne Van. Loggenberg, "Computer Vulnerability Risk Anakysis", Master in Science Dissertation, Univ. Rand Afrikaans, May 2003

[8] C. Marnewick, L. Labuschagne, "A Security Framework for an ERP System", Univ. Johannesburg, 2006, South Africa.

[٩] سيد علي. فيروزآبادي "تجربيات پياده‌سازي محصول ERP شركت SAP در گروه صنعتي ايران خودرو"، دومين همايش بررسي تجربيات پياده‌سازي سيستم‌هاي برنامه‌ريزي منابع سازمان، دانشگاه علم و صنعت ايران، تهران، ايران، آبان، ١٣٨۶.

[١٠] احمد. اكبري، "ذوب‌آهن اصفهان برترين شركت ايميدرو در حوزه ICT"، اولين همايش سالانة هم‌انديشي مديران و كارشناسان ICT سازمان توسعه و نوسازی معادن و صنایع معدنی ایران (ایمیدرو)، تهران، ايران، بهمن، ١٣٨۶.

[١١] مرتضي. نخعي، "تجربيات پياده‌سازي ERP در ذوب‌آهن اصفهان"، اولين همايش تجربيات پياده‌سازي سيستم‌هاي برنامه‌ريزي منابع سازمان، دانشگاه علم و صنعت ايران، تهران، ايران، آبان، ١٣٨۵.

[۱۲] سيد مهدي. سيف‌هاشمي، "تجربيات پياده‌سازي ERP در شركت ملي صنايع مس ايران"، اولين همايش تجربيات پياده‌سازي سيستم‌هاي برنامه‌ريزي منابع سازمان، دانشگاه علم و صنعت ايران، تهران، ايران، آبان، ۱۳۸۵.

[۱۳] محمدحسين. قميان، "ERP در صنعت برق: روش، تجربيات و دستاوردهاي انتخاب راه‌حل ERP در شركت برق منطقه‌اي آذربايجان"، دومين همايش بررسي تجربيات پياده‌سازي سيستم‌هاي برنامه‌ريزي منابع سازمان، دانشگاه علم و صنعت ايران، تهران، ايران، آبان، ۱۳۸۶.

[۱۴] كاظم. آيت‌الهي، "از انتخاب تا پياده‌سازي ERP"، تكفا، سال پنجم، شمارة ۳ و ۴، تير و مرداد ۸۶.

[۱۵] محسن. رياستيان، "اجرايي شدن كامل ماژول‌هاي SAP در توگا"، دومين همايش بررسي تجربيات پياده‌سازي سيستم‌هاي برنامه‌ريزي منابع سازمان، دانشگاه علم و صنعت ايران، تهران، ايران، آبان، ۱۳۸۶.

[۱۶] علي‌اكبر. جلالي، سعيد. روحاني، محمد امين. زارع، "مديريت سيستم‌هاي برنامه‌ريزي منابع سازمان"، انتشارات شركت خدمات انفورماتيك راهبر، ۱۳۸۶.

[۱۷] آرش. شاهين، مهيار. نظري، سعيده. بقائي، "بررسي تطبيقي عوامل كليدي موفقيت در استقرار ERP و BPR"، چهارمين كنفرانس بين المللي مديريت فناوري اطلاعات و ارتباطات، تهران، ۲۹ و ۳۰ بهمن ۱۳۸۶.

[۱۸] مصطفي. هاشم‌زاده، "برنامه‌ريزي منابع سازماني چيست؟"، پايگاه جامع مهندسي صنايع ايران، http://www.ieir.ir/Cat/23.aspx، (Visited on 2008-05-12).

[19] E.A. Steyn, "A Framework for Assessing Enterprise Resource Planning Systems", Magister Commercii Dissertation, Univ. Afrikaans, October 2004.

[20] Carl. Dahlen, Johan. Elfsson, "An analysis of the current and future ERP market", Master's Thesis, The Royal Instiitute of Technology, Stokholm, February 1999.

[۲۱] محمد. حسني، "آشنايي با سيستم‌هاي برنامه‌ريزي شده با تكيه بر ERP"، سازمان توسعه و نوسازي معادن و صنايع معدني ايران، تهران، ۲۵ شهريور ۱۳۸۲.

[22] Robert. Farrington, "Oracle Applications Concepts", Releas 12, Part No.B31450-01, December 2006.

[23] Steve. Latropoulos, "Microsoft Business Solutions Navision Integration Guide", August 2005.