دانشگاه آزاد اسلامی

واحد دانشگاه علوم و تحقیقات تهران

پروژه پایان ترم درس معماری نرم افزار پیشرفته

طراحی معماری سامانه پرداخت بر اساس ویژگی های کیفی

استاد

دکتر علی رضایی

تهیه کننده

مهدی شعبانی

زمستان ۹۵

Mh.shaabani@gmail.com

مقدمه

در این مستند سعی شده نمونه ای از معماری یک سیستم نرم افزاری با رویکرد استناد بر ویژگی های کیفی را ارایه کنیم. این سند در واقع نمونه ی مختصری از یک معماری Attribute Driven Design است که در آن فرایند های نمونه، بر اساس خصوصیات کیفی تجزیه شده اند.

در هر تکرار از رویکرد فوق تعدادی تاکتیک برای رسیدن به هدف انتخاب می شود. روال به این شکل است که مجموعه پیشران های معماری را انتخاب میکنیم و ماژولی را برای تجزیه، هدف قرار می دهیم. پیشران ها را اولویت بندی می کنیم و تاکتیک هایی را ارایه کرده و وظایف را برای ماژولها شرح می دهیم. سعی شده در بخش هایی از نمایه های فرایند توسعه RUP متناسب با صورت مسأله فرضی مان برای بیان ساختار استفاده کنیم.

برای این سند یک سیستم پرداخت امن را به عنوان پروژه نرم افزاری در نظر می گیریم و با رویکرد ADD سعی در ارایه ی طراحی می کنیم. با توجه به دامنه ی یک پروژه ی درسی تمام ماژولها و فعالیت ها و ارتباطات را پوشش نمی دهیم و سعی می کنیم چند ماژول اصلی و ساختار ضروری سیستم ، ارتباطات و چند ویژگی کیفی را به عنوان نگاشت مطالب درسی ارایه شده توسط استاد عزیز اقای دکتر علی رضایی را مستند کنیم.

تعاریف و مفاهیم

شبکه کنونی بانکی کشور مبتنی بر تراکنش های آنلاین است که در آن برای راحتی کاربران در هنگام ورود به خدمات پرداخت، یک کارت PVC در نظر گرفته شده است که دارای نوار مگنت بوده و شماره حساب و شماره بانک عامل حساب فرد در آن نوار به صورت آشکار درج شده است و فقط به دلیل پرهیز از خطای ورود دستی اطلاعات، اطلاعات از نوار مگنت آن کارتها خوانده می شود. این روش بیش از ۴۰سال قدمت داشته و جوابگوی پرداختهای نوین امروزی نیست.

در عصر اراتباطات امروزی، سرعت و راحتی در کنار امنیت از پارامترهای حیاتی فعالیتهای حوزه فینتک است. در حوزه پرداخت خرد مفهوم TAP & PAY بوجود آمده است که در آن برای راحتی و سرعت عمل در پرداختهای خرد، از دریافت اطلاعات اضافی از فرد مانند رمز کارت پرهیز می شود. این پرداختها تنها با قرار دادن مدیای پرداخت اعم از کارت هوشمند و یا تگ های RFID بر روی کارتخوانهای ترمینالها بدون ورود اطلاعات اضافی صورت می گیرد.

اکوسیستم لازم برای چنین پرداختهایی از نرم افزار تعبیه شده در کارت، سخت افزار ترمینالها ونرم افزار تعبیه شده در آنها(پذیرنده) ، سرویس های تجمیع، تفسیر، تسهیم و تسویه در سمت سرور تشکیل شده است. قالب پیاده سازی برنامه های کارت، پیاده سازی اپلت است. اپلت ها برنامه های کوچک و بهینه ای هستند که برای اجرا در پردازنده ضعیف کارتهای هوشمند تهیه می شوند.

عمل Debit به معنی کسر مبلغ از مقدار موجود در کارت یا حساب و عمل Credit به معنی افزودن مبلغ به موجودی فعلی کارت یا حساب فرد است.

در این پروژه طراحی اجمالی بر روی پرداخت آنلاین و آفلاین مبتنی بر کارتهای هوشمند RFID و مولفه های اصلی سیستم متولی آن ارایه خواهیم کرد.ویژگی های عمده سیستم به شرح زیر متصور است:

امکانات کارت: محدودیت های سقف شارژ ، محدودیت های سقف تراکنش روزانه، امنیت، سادگی کار و راحتی، سرعت

امکانات پذیرنده: جمع آوری و نگهداری و ارسال مناسب تراکنش ها، امنیت در ارتباط با سرور مرکزی، سادگی و UserFriendly بودن

امکانات سیستم تسهیم و تسویه: یک وب برای دسترسی کلیه ذی نفعان سیستم با دسترس پذیری بالا , امکان مشاهده ی انواع گزارش های تراکنش ها، امکان انجام عملیات تسویه بانکی به موقع و بی اشتباه و امکان رهگیری تراکنش ها و کشف مغایرات

قطعا موارد مطروحه گزینشی است و تمامی جزییات و فعالیتها و عناصر مورد اشاره قرار نمی گیرد چراکه هدف نگاشت مطالب درسی ارایه شده طول ترم با نمونه فرضی از یک پروژه است.

معرفی ذی نفعان پروژه

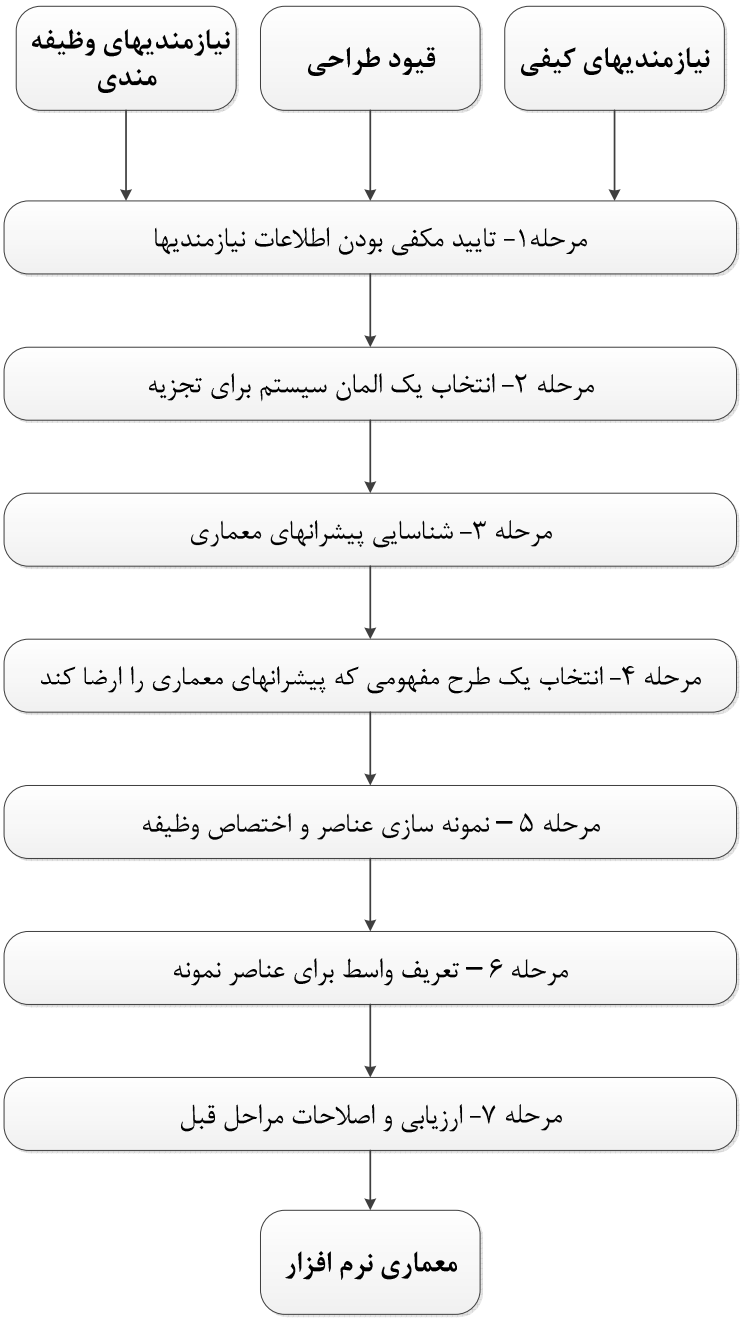
فرض می شود یک سیستم پرداخت خرد مبتنی بر کارت هوشمند در بستر online و offline داریم. در این سیستم یک موسسه مالی مثلا بانک شهر، به عنوان عامل صدور کارت کیف پول خرد الکترونیکی، یک شبکه پذیرندگی مثلا PSP فناوا، یک مجموعه فروشندگان اجناس خرد قیمت، مثلا نانوایی ها، تاکسی ها و یک جامعه دارنده ی کارت به عنوان پرداخت کننده پول خرد و دریافت کننده سرویسهای شهری متداول امروزی، به عنوان ذی نفعان متصور هستند .

ذی نفعان	توضیح
بانک شهر	بازکننده حساب برای مردم منفعت از طریق رسوب پول سپرده ی مردم منفعت از طریق افزایش ضریب نفوذ حساب های بانکی اش در جامعه
PSP فناوا	فراهم کننده ی POS و ترمینال ها برای کسب و کارها ی درگیر پرداخت خرد مثل نانوایی و تاکسی ها منفعت از طریق اخذ درصدی کارمزد از هر تراکنش صورت گرفته در ترمینال های شبکه خودش
نانوایی ها و تاکسی ها	فراهم کننده خدمات شهر از قبیل حمل و نقل مردم و یا فروش نان روزانه مردم منفعت از طریق آسان سازی پرداخت مشتریان و کاهش زمان سرویس دهی و افزایش بهره وری سرویس های ارایه شده
مردم	خریداران خدمات شهر که مجبور هستند برای دریافت خدمات کوچک روزانه درگیر تهیه پول خرد باشند منفعت از طریق سادگی پرداخت، کاهش زمان، مصوب بودن هزینه های پرداختی و جلوگیری از مجادلات و دعاوی

خواسته های ذی نفعان فوق در معماری این پروژه تاثیر گذار است.(بحث ABCاز درس این ترم)

طراحی معماری

برای طراحی معماری از گام های تعریف شده در ADD استفاده میکنیم.



ADD یک روش طراحی معماری به صورت Iterative است که سعی می کند معماری را با توجه به چند پیشران مهم و اولیه از جمله نیازمندی های وظیفه مندی، خصوصیت کیفی و قیود شکل دهد. در این روش بر اساس چند نیازمندی پر اهمیت اولیه، معماری شکل گرفته و سایر نیازمندی ها بر حول آنها توسعه می یابند. در ادامه به روند کار در تکرار اول از روش ADD برای طراحی معماری می پردازیم.

انتخاب مجموعه پیشران های معماری

مجموعه پیشران های معماری را بر اساس نیازمندی وظیفه مندی Functional ، خصوصیات کیفی و قیود حاکم تشکیل می دهیم.

خصوصیات کیفی یا Non-Functional Requirements

قابلیت دسترس پذیری

پذیرنده های این سیستم در دوحالت Offlineو Online متصور هستند. در حالت Offline هر پذیرنده باید سرویس خرید را به صورت مناسب و باکیفیت در تمام طول شب و روز در دسترس پرداخت کننده ها قرار دهد به گونه ای که تراکنش ها با سرعت بالا و بدون خطا Failure، انجام پذیرد و مبلغ مورد نظر کسر شود. در حالت Online نیز پذیرنده باید سرویس خرید و سرویس شارژ کارت را به صورت مناسب و بدون خطا و سریع فراهم کرده و تراکنش ها با موفقیت صورت پذیرند. سرویس تجمیع تراکنش ها در مرکز نیز باید به صورت مناسب دسترس پذیر باشد تا پذیرنده ها به موقع و طبق دوره ی تسویه Config شده در آنها، با ارتباط با سرویس تجمیع، تراکنش های ذخیره شده ی خود را ارسال کنند. سامانه وب نیز باید دسترس پذیر باشد تا در هر لحظه ذی نفعان سیستم با اکانت خود وارد شده و فعالیت های مجاز خود مانند گزارش گیری ها را انجام دهند.

خصوصیات کیفی مورد نیاز منطبق بر قابلیت دسترس پذیری در جدول زیر آورده شده اند.

شناسه سناریو: SI_1	
عنصر سناریوی کیفی	**مقادیر**
منبع	صاحب کارت به هنگام پرداخت به وسیله کارت این تحریک را ایجاد می کند
محرک	ترمینال پذیرنده عمل کسر مبلغ را نتواند انجام دهد
محصول	نرم افزار ترمینال
محیط	شرایط عملیاتی نرمال سیستم
پاسخ	شکست تراکنش تشخیص داده شود و پیغام مناسب مبنی بر تکرار تراکنش به کاربر داده می شود
معیار اندازه گیری	در مدت حداکثر ۳۰۰ میلی ثانیه , Ok Ack بین کارت و پذیرنده تبادل شده باشد و مبلغ موجودی به میزان خرید کاهش یافته باشد

شناسه سناریو: SI_2	
عنصر سناریوی کیفی	مقادیر
منبع	پذیرنده در ساعت ۱۲ شب سرویس تجمیع تراکنش های سرور را فراخوانی کند
محرک	سرویس، مجموعه تراکنش های ارسالی را ناقص دریافت کند یا اصلا متد status سرویس مقدار Not OK برگرداند
محصول	سرویس تجمیع تراکنش
محیط	شرایط عادی عملیاتی و سر رسید زمان تسویه ی دوره ای
پاسخ	بالا نبودن سرویس کشف شود و پیغام مناسب برگردانده شود و مجددا عمل retry به صورت خودکار انجام پذیرد
معیار اندازه گیری	هر ۱۰۰۰ تراکنش در قالب یک xml حداکثر ظرف ۲ ثانیه به مرکز ارسال شده و Ok ACK دریافت شود

شناسه سناریو: SI_3	
عنصر سناریوی کیفی	مقادیر
منبع	سرویس کنترل دسترسی سامانه وب ذی نفعان
محرک	یک فروشنده نتواند وارد پروفایل کاربری خود شود
محصول	سامانه وب مدیریت ذی نفعان
محیط	شرایط عادی کار سیستم با ترافیک بالای کاربران
پاسخ	تشخیص اشکال و نمایش پیغام مناسب و فوروارد کردن کاربر به صحفه ی مناسب
معیار اندازه گیری	کاربر بعد از وارد کردن نام کاربری و گذرواژه و مقدار کپچا، ظرف کمتر از یک ثانیه وارد صفحه اصلی پروفایل کاربری خود شود

قابلیت امن بودن

اپلت ePurse موجود در کارت که قابلیت نگهداری مقدار موجودی پول و عملیات شارژ و خرید را بر عهده دارد باید از سطح امنیت بالایی برخوردار باشد. پشتیبانی از استاندارد های امنیتی از قبیل FIPS140-2, مولد تصادفی واقعی و مولد کلیدهای رمزنگاری سخت افزاری و طول کلید مناسب در الگوریتم ها از نیاز های امنیتی کارت هوشمند هستند .

مقادیر پول و تراکنش ها باید با پروتکل های امن سازی دارای ویژگی های قابلیت عدم انکار و دستنخوردگی و محرمانگی باشند تا از امکان جعل پول جلوگیری شود. سرویس تجمیع تراکنش ها باید دارای پارامتر های احراز هویت باشد و ترمینال

ارسال کننده تراکنش ها را ارزیابی کرده و فقط به ترمینال های مجاز اجازه ارسال تراکنش دهد. سامانه وب تسهیم نیز باید طبق پیشنهادات OWASP امن سازی شود تا نفوذ گر نتواند اقدام به مشاهده گزارشها و احیانا دستکاری آنها کند.

شناسه سناریو: SI_11	
عنصر سناریوی کیفی	مقادیر
منبع	نرم افزار ترمینال پذیرنده
محرک	نرم افزار ترمینال درخواست ارسال تراکنش های تجمیع شده در حافظه ترمینال به سرویس تسویه را دارد
محصول	سامانه تسهیم و تسویه پرداخت خرد
محیط	شبکه ارتباطات پذیرندگی ها
پاسخ	سرویس باید پذیرنده را احراز هویت کند و از تمامیت یا دستخوردگی داده های ارسالی اطمینان حاصل کند
معیار اندازه گیری	تعداد تلاشهای ناموفق از طریق فراخوانی های ناشناس باید صفر باشد

شناسه سناریو: SI_12	
عنصر سناریوی کیفی	مقادیر
منبع	کارت ePurse
محرک	ترمینال نامعتبر سعی در شارژ کردن کارت کند
محصول	کیف پول خرد الکترونیکی
محیط	فرایندهای متداول روزمره یا محیط های ازمایشگاهی حمله
پاسخ	تراکنش شارژ نامعتبر، باید Faild شود و بعد از چند تکرار غیر مجاز باید کارت بلوکه یا قفل شود
معیار اندازه گیری	میزان مغایرت مبالغ شارژ شده بین کارت ها و سرور مرکزی باید صفر باشد و عملا امکان جعل شارژ و جعل پول مجاز نباشد

قابلیت اصلاح پذیری Modifiability

با توجه به تغییرات پارامترهای شبکه پرداخت، اعم از مبالغ کارمزدها، بروزرسانی ترمینال ها، رفع خرابی POS ها و امثال آنها باید مولفه های سیستم قابلیت اصلاح داشته باشند. مثلا در صورت نیاز به نسخه جدید اپلت کارت باید بتوان با اولین تماس کارت به یک پذیرنده، اپلت آن را بروزرسانی کرد یا مثلا در صورت افشای کلید های Credit و Debit باید بتوان SAM های ترمینال ها را اصلاح کرده و فرایند تراکنش ها را با وضعیت جدید ادامه داد.

امکان تغییر محدودیت های تراکنش روزانه، سقف هر تراکنش، میزان موجودی حداکثری یک کارت و پارامترهای حیاتی این چنینی دیگر، نیز باید قابلیت اصلاح و تغییرات در طول چرخه حیات سیستم را داشته باشند.

شناسه سناریو: SI_21	
عنصر سناریوی کیفی	مقادیر
منبع	بانک صادر کننده کارت
محرک	درخواست تغییرات درصد کارمزد پذیرنده
محصول	اپلت درونی کارت و نرم افزار ترمینال پذیرنده
محیط	در فاز عملیاتی نرمال در ابتدای سال مالی جدید
پاسخ	بررسی اینکه آیا تغییرات قابل اجرا در سیستم هست یا نه , ارسال فایل CAP حاوی نصاب اپلت ePurse از طریق شبکه به ترمینال و از ترمینال به کارت ها
معیار اندازه گیری	درصد کارمزد تراکنش ها بعد از بروزرسانی مطابق با مبلغ جدید باشد

شناسه سناریو: SI_22	
عنصر سناریوی کیفی	مقادیر
منبع	واحد طراحی پروتکل و شخصی سازی
محرک	درخواست بروز رسانی کلید Debit در ماژول SAM موجود در ترمینال ها ی شهر تهران به دلیل افشای کلید Debit جاری
محصول	ماژول SAM مربوط به debit در ترمینال ها
محیط	شبکه ی پرداخت و ترمینال های PSP در محدوده تهران
پاسخ	بروز رسانی امن کلیدها طی مراسم تشریفات کلید از طریق کلید برقراری SecureExchange و عملیات Key Agreement براساس پروتکل دیفی هلمن، انجام تراکنش تست و ارزیابی به عنوان ACK
معیار اندازه گیری	تراکنش تستی جدید باید دارای Cryptogram تولید شده با کلید جدید مورد انتظار باشد.

قابلیت استفاده

این ویژگی به میزان سادگی کار با سیستم اشاره دارد. اگرچه سطح خود اگاهی دارندگان کارت بسیار متنوع است و در بعضی موارد، بضاعت فنی بالا و بعضی موارد پایین است، با این حال نباید سادگی فراموش شود. داشتن واسط کاربری ساده روی ترمینال ها و وب سایت و نمایش پیغام های گویا و غیر تخصصی به صاحب کارت و صاحب فروشگاه دارای پذیرنده، وجود راهنما در تمام سناریو های سیستم و عدم نیاز به وارد کردن اطلاعات خاص در لحظه تراکنش از مصادیق قابلیت استفاده بالا هستند.

شناسه سناریو: SI_31	
عنصر سناریوی کیفی	مقادیر
منبع	دارنده کارت
محرک	کاربر قصد دارد هزینه خرید کالا را بپردازد
محصول	سیستم پرداخت
محیط	محیط مصرف کننده سیستم یعنی Merchant ها
پاسخ	فرایند به گونه ای طراحی و اجرا شده باشد که فرد تنها با قرار دادن کارت روی کارتخوان POS , بدون کوچکترین عمل اضافی پرداخت را انجام دهد و هزینه کسر شده و هزینه موجودی باقی مانده را در قالب رسید چاپی دریافت کند
معیار اندازه گیری	مبلغ مورد انتظار خرید از کارت کسر شده باشد و موجودی مورد انتظار نیز در رسید ثبت شده باشد نه اینکه مبالغ مغایر باشند

شناسه سناریو: SI_32	
عنصر سناریوی کیفی	مقادیر
منبع	کاربر سیستم- ذی نفعان
محرک	صاحب شرکت تاکسیرانی قصد دارد در سایت تسهیم و تسویه، مشخصات یکی از رانندگان و شماره حساب و درصد کارمزد او را ثبت کند
محصول	سامانه تسهیم و تسویه
محیط	محیط عملیاتی یا وب سایت سامانه
پاسخ	به سادگی بتواند لینک صفحه ثبت کاربر، ثبت POS جدید و ثبت مشخصات ذی نفع جدید را پیدا کرده و به سادگی داده های مورد نیاز را وارد و ثبت کند
معیار اندازه گیری	میزان زمان طول کشیده که فرد برای ثبت ذی نفع جدید صرف کرده و میزان خطایی که در وارد کردن مشخصات ذی نفع داشته است

کارایی

زمان انجام تراکنش، در صف های طولانی مثلا اتوبوس یا نانوایی ها بسیار حیاتی است. اگر قرار باشد سیستم کارایی پایینی داشته باشد وجود این سیستم مشکل پرداخت های خرد سنتی را حل نکرده است. پس باید در کمتر از۲۰۰ میلی ثانیه و بدون خطا فرد کارت خود را TAP کرده و هزینه پرداخت شود و نوبت فرد بعدی فرا برسد.

شناسه سناریو: SI_33	
عنصر سناریوی کیفی	مقادیر

منبع	صاحب کارت که در صف نانوایی نوبتش رسیده است
محرک	تراکنش پرداخت یا Debit انجام می شود
محصول	سیستم پرداخت
محیط	محیط عملیاتی نرمال
پاسخ	هزینه پرداخت می شود و پیغام مناسب نمایش داده می شود
معیار اندازه گیری	مدت زمانی که صاحب کارت منتظر پاسخ در نمایشگر POS بوده و تعداد دفعاتی که لازم بود تا تکرار کند

شناسه سناریو: SI_34	
عنصر سناریوی کیفی	**مقادیر**
منبع	ترمینال اقدام به ارسال تراکنش هایش برای تسویه می کند
محرک	سرویس تجمیع ، تسهیم، تسویه فراخوانی می شود
محصول	سیستم پرداخت
محیط	عملیاتی
پاسخ	باید با سرعت مناسب و سر وقت و طبق زمان بندی قبلی پول ها ی Merchant به حسابش واریز شود.
معیار اندازه گیری	از لحظه شروع عملیات تسویه باید ظرف ۱۰ ثانیه پول به حساب صاحب پذیرنده ریخته شود

قابلیت حمل

قاعدتا بعضی از مشاغل خرده فروش به صورت سیار هستند مثلا روزنامه فروشی یا تاکسی های دارای تاکسی متر.

قابلیت حمل، اجازه می دهد عمل پرداخت و پذیرندگی در یک خودروی مسافرکشی هم صورت بپذیرد. بنابراین باید ارتباطات سیار برای ارسال تراکنش و تسویه برای پذیرنده های سیار نیز موجود باشد.

شناسه سناریو: SI_41	
عنصر سناریوی کیفی	**مقادیر**
منبع	صاحب کارت
محرک	می خواهد هزینه تاکسی بین مبدا و مقصد را بپردازد
محصول	سیستم پرداخت
محیط	محیط عملیاتی درون تاکسی
پاسخ	مبلغ کرایه به سادگی از کارت فرد کسر می شود و رسید تحویل شود
معیار اندازه گیری	تعداد کل سفر های دارنده ی کارت / تعداد دفعات پرداخت موفق در تاکسی= معیار

نیازهای وظیفه مندی یا Functional

نیاز های وظیفه مندی جهت دهی معماری برای معمار را فراهم می کند.

در زیر نیازهای Functional شناسایی شده برای سیستم پرداخت خرد را ارایه کنیم.

مجموعه نیازهای وظیفه مندی	توضیح
وظیفه مندی های مربوط به اپلت کارت	احراز هویت کردن ترمینال پذیرنده عملیات Debit امن عملیات Credit امن عملیات Cash out امن عملیات لاگ برداری از تراکنش ها شمارنده داخلی تراکنش ها
وظیفه مندی ترمینال پذیرنده	منوی تنظیمات ماژول ارتباطات شبکه برای ارتباط با مرکز ماژول Secure PIN PAD ماژول نرم افزاری ارتباط با SAM اسلات فیزیکی SAM نرم افزار مولد APDU های تراکنش های مختلف عملیات لاگ برداری
وظیفه مندی های سرویس تسویه	وب سرویس دریافت تراکنش ها تابع احراز هویت فرستنده تراکنش وب سرویس تابع برقراری تونل امن تراکنش های وب سرویس ارسال تراکنش های دریافتی به بانک اطلاعاتی مخزن تراکنش ها انجام زمان بندی واریز مبالغ تسویه حساب
وظیفه مندی های وب تسهیم و تسویه	مدیریت کاربران ثبت POS و انواع پذیرنده ثبت ذی نفعان گزارش آماری تراکنش ها به ازای سازمان ها و ذی نفعان مختلف اصلاح و تغییرات در کارمزد ها و سهم ذی نفعان

قیود Constraints

در زیر قیدهای متصور بر فعالیتهای سیستم را ذکر می کنیم:

#Cons1 نرم افزار ترمینال ها فقط بر روی ترمینال های منطبق بر استاندارد EMV قابل نصب و اجرا هستند.

#Cons2 کارت مورد استفاده از نوع جاوا کارت نسخه ۲ . ۲ . ۲ می باشند.

#Cons3 الگوریتم های مورد استفاده در تراکنش ها متقارن باشند.

#Cons4 عملیات تولید شارژ فقط در HSM مرکزی صورت پذیرد.

#Cons5 طول کلید های مورد استفاده حداقل ۲۵۶ بیت باشد.

#Cons6 پذیرنده ها باید حتما از SAM ماژول های سخت افزاری استفاده کنند.

توافق بر سر نیازمندی های مکشوفه

در این مرحله نیازمندی های Functional , خصوصیات کیفی و قیود کشف شده در فاز اول فرایند ADD را به تایید ذی نفعان می رسانیم. در این پروژه فرض می شود ذی نفعان مفروض، تایید کرده اند.

انتخاب ماژول برای تجزیه

ما کل سیستم را انتخاب میکنیم.

اولویت بندی پیشران های معماری

در این مرحله پیشران های پروژه را اولویت بندی می کنیم. این اولویت بندی بر اساس نیاز های وظیفه مندی، خصوصیات کیفی و قیود شکل گرفته است.

بر اساس تحلیل و تشخیص معمار، اینطور فرض می شود که خصوصیات کیفی قابلیت دسترسی، امنیت بالا و کارایی و قابلیت تغییر نسبت به بقیه ویژگی ها اهمیت بیشتری دارند و لذا بیشتر مورد توجه قرار میگیرند.

در جدول زیر اولویت بندی و میزان پیچیدگی ها آورده شده است.

پیشران معماری	اهمیت	پیچیدگی ساخت
قابلیت دسترسی	بالا	پیچیده
امنیت	بالا	پیچیده
کارایی	بالا	متوسط
قابلیت اصلاح	متوسط	متوسط
قابلیت حمل	متوسط	متوسط

قید Cons1	کم	کم
قید Cons2	کم	کم

انتخاب تاکتیک های معماری

اکنون به ارایه ی تاکتیک های متناظر با ویژگی های کیفی فوق می پردازیم و سایر خصوصیات کیفی را متناسب با آنها توسعه می دهیم.

شرح تاکتیک های مورد استفاده

اکنون قصد داریم در مورد انتخاب تاکتیک های مناسب و مورد نیاز مان تصمیم گیری کنیم.

تحقق قابلیت دسترس پذیری

در این بخش تاکتیک های مورد استفاده و الگوی پیشنهادی معمار برای خصوصیت کیفی دسترس پذیری ذکر گردیده است.

دسترس پذیری	استفاده از تاکتیک Sanity checking	با توجه به اینکه تراکنش ها دارای طول های حداکثر۱۵۰ بایتی هستند و فرمت encoding آنها به صورت base64 هست پس با استفاده از تاکتیک sanity checking در صورت مشاهده رشته های غیر base64 یا طول های خیلی کوچک یا خیلی بزرگ مثلا بیشتر از ۱۵۰ بایت، الگوی خطا فرض گردیده و نقص سیستم تشخیص می دهیم.
	استفاده از تاکتیک ROLLBACK	با نگهداری state های حیاتی تراکنش ها، اگر تراکنش های متوالی با اشکال برخورد عمل Rollback و برگرداندن سیستم به آخرین وضعیت نرمال را فراهم می کنیم.
	استفاده از تاکتیک افزونگی فعال	با توجه به فراوانی POS های متصل به سرویس تسویه و امکان همپوشانی دوره های تسویه و همزمانی آنها از سه سرور به صورت Redundant به صورت Load balance شده استفاده می کنیم تا همزمانی احتمالی تسویه ها باعث ایجاد اختلال در سرویس تسویه نشوند.
	استفاده از تاکتیک تراکنش	تراکنش ها در کارت به صورت بلاک های Atomic پیاده سازی می شوند تا در صورت اختلال در هر قسمت از فرایند تراکنش,کلیه عملیات قبلی نیز به حالت قبل برگردانده شوند و ناهمخوانی در وضعیت های درونی کارت و حساب های سمت سرور پیش نیاید.

	استفاده از تاکتیک Self Test	در POS ها یک سرویس Self Test برای تست درایور PCSC کارتخوان و SAM ها و نیز وضعیت کارتخوان contactless طراحی و پیاده سازی می شود تا دایما از آماده بودن کارتخوان غیر تماسی اطمینان حاصل شود. زیرا در پرداخت نوع TAP & PAY واسط غیر تماسی کارتخوان ها مورد استفاده قرار می گیرد و صحت کارکرد آن بسیار حیاتی است.
	استفاده از تکنیک های SoftWare Upgrade	برای بروز رسانی های ماژول های پذیرنده ها استفاده می کنیم.
	استفاده از تاکتیک Ping/Echo	برای استعلام وضعیت ارتباط POS ها با سرویس تجمیع تراکنش و تسویه، در بازه های زمانی یک ساعته عمل Ping سرور تسویه به صورت خودکار انجام می شود.

تحقق ویژگی امنیت

در این بخش تاکتیک های مورد استفاده و الگوی پیشنهادی معمار برای خصوصیت کیفی امنیت ذکر گردیده است.

امنیت	تاکتیک رمزنگاری داده ها	اقلام حساس از قبیل مقادیر شارژ و موجودی حساب ها به صورت رمز شده در محل های انباشت یا در بستر ارتباطی مورد استفاده قرار می گیرد .
	تاکتیک احراز هویت	کاربران ذی نفع سامانه برای ورود به وب تسهیم، احراز هویت می شوند. در ضمن پذیرنده هایی که به سرویس تجمیع تراکنش متصل می شوند ابتدا احراز هویت می شوند و در روش مبتنی بر Challenge/ Response با SAM موجود روی آن یک عمل احراز هویت صورت می گیرد.
	تاکتیک اعتبار سنجی	تراکنش ها به امضای دیجیتال مجهز هستند و در صورت ارسال به مرکز، اعتبار سنجی می شوند تا تراکنش های نا معتبر رد شوند.
	تاکتیک تشخیص حملات	پیاده سازی یک تحلیل گر درخواست ها و تراکنش های انجام شده روی سیستم
	محدود کردن دسترسی به داده ها	در صورت تکرار تلاش ناموفق برای دستیابی کاربران غیر مجاز به پروفایل کاربران در وب تسهیم بعد از چند شکست متوالی اکانت

		مربوطه بلاک می شود. دسترسی به عملیات SAM های پذیرنده ها از طریق مکانیزم امنیتی مبتنی بر ۳ کلید 3 DES صورت می پذیرد.
	استفاده از تاکتیک اطلاع رسانی یا Inform Actors	ارسال SMS به صاحب کارت در صورت تراکنش کسر مبلغ بیشتر از ۵۰۰۰ تومان برای اطلاع رسانی به صاحب آن که در صورت برداشت غیر مجاز از حسابش متوجه شود.
	استفاده از تاکتیک نگهداری از شواهد برای بازرسی	نگهداری از log فعالیت های سیستم و طبقه بندی این فعالیت ها بر اساس سه رنگ سفید، زرد و قرمز که بتوان بر اساس آنها تحلیل و ارزیابی فعالیت های نامتعارف را انجام داد.

تحقق ویژگی کیفی کارایی

در این بخش تاکتیک های مورد استفاده و الگوی پیشنهادی معمار برای خصوصیت کیفی کارایی ذکر گردیده است.

کارایی	استفاده از تاکتیک افزایش منابع در دسترس	اختصاص سرور با تعداد CPU و حافظه ی بیشتر تنظیمات مناسب مربوط به اندازه حافظه CACHE موقت سرویس دهنده وب و افزایش پهنای باند شبکه جهت انتقال
	استفاده از تاکتیک نگهداری چندین کپی از داده ها	برای جلوگیری از ریسک از بین رفتن تراکنش ها، تراکنش ها در ترمینال به صورت دسته ای ذخیره می شوند و در عین حال هر کارت ۴۰ تراکنش آخر خود را نیز در درون خود ذخیره می کند که درصورت از بین رفتن POS به هر دلیلی می توان تراکنش های هر کارت را (۴۰ تراکنش آخر) بازیابی و رسیدگی کرد. اما هدف اصلی از این کار افزایش سرعت عمل کارت در محاسبه تراکنش های وابسته به تراکنش قبلی است که برای این کار تراکنش قبلی را از ترمینال نمی گیرد بلکه از حافظه خود میخواند(مثلا در عمل Cash out).

تحقق ویژگی کیفی قابلیت اصلاح

هدف تغییرپذیری یا اصلاح، کنترل زمان ، هزینه پیاده سازی ، تست و استقرار سیستم است. درمورد سیستم پرداخت , تغییر در پارامتر های عملیاتی node های شبکه PSP در اسرع وقت, اهمیت بالایی دارد.

در این بخش تاکتیک های مورد استفاده و الگوی پیشنهادی معمار برای خصوصیت کیفی قابلیت اصلاح ذکر گردیده است.

	تاکتیک سازگاری داده ها	برای این منظور از پروتکل ها و تکنولوژی های معروف و استاندارد

قابلیت اصلاح	با استاندارد ها	استفاده می کنیم. مثلا از قالب استاندارد xml جهت تبادل داده ها استفاده می کنیم. از تکنولوژی مبتنی بر SOAP استفاده می کنیم.
	تاکتیک حفظ انسجام معنایی	استفاده ازمولفه سازی جهت دسته بندی مولفه هایی که انسجام معنایی را به جود آورند.
	تاکتیک حفظ واسط های موجود	برای حفظ واسط ها و عدم انتشار نامطلوب تغییرات در عملیات کلاس ها , الگوهای بسیار وجود دارد. استفاده از الگوهای طراحی Factory، Abstract Factory، Facadeو Adaptor بسیار سودمند است. استفاده از الگوی معماری Layer و MVC نیز جهت جداسازی سطوح مختلف وظیفه مندی سیستم از جمله واسط کاربری منطق برنامه و دسترسی داده ها در این خصوص سودمند است.
	تاکتیک استفاده از فایل های پیکر بندی	این تاکتیک در راستای امکان اعمال تغییرات در زمان اجراست. در ترمینال ها باید امکان تغییر آدرس وب سرویس تجمیع در سمت سرور وجود داشته باشد . در فایل های Config باید امکان تغییر مشخصات ترمینال از قبیل شماره و سریال وجود داشته باشد.

معرفی مولفه های سیستم

در زیر لیست عناصر مورد نیاز این سیستم مشخص شده است.

- *مؤلفه مدیریت خطا*
- *مؤلفه ارتباط با کارتخوان*
- *مؤلفه تولید APDU*
- *مؤلفه مدیریت لاگ*
- *مؤلفه مدیریت کنترل دسترسی*
- *مؤلفه WS client*
- *مؤلفه مدیریت تراکنش*
- *مؤلفه تشخیص جرم*
- *مؤلفه واسط کاربری*
- *مؤلفه چاپ*
- *مؤلفه ارتباطات شبکه*

معرفی ماژول ها و تشریح هر یک از دید های معماری پیشنهادی

اکنون پس از انتخاب تاکتیک های معماری و الگوهای پیشنهادی جهت ارضای خصوصیات کیفی آنها را با هم ترکیب می کنیم و معماری پیشنهادی را طراحی می کنیم. ترکیب و اعمال الگوها در سطوح مختلف معماری پیشنهادی با توجه به اولویت خصوصیات کیفی است. پس از طراحی معماری، آنرا با دید های مختلف معماری نمایش می دهیم.

ما از دید *های* لایه، دید *استقرار* و دید *کلاس* (برای نمایش جزییات داخل مؤلفه ها)، دید *تجزیه ماژول* و دید *کد* جهت نمایش معماری پیشنهادی خود استفاده خواهیم کرد.

در واقع آنچه که معماری پیشنهادی را شکل داده است الگوهایی است که در راستای تحقق تاکتیک ها استفاده شده است. بالطبع، الگو ها نیز در راستای پوشش دادن خصوصیات کیفی و نیازمندی های کار کردی انتخاب یا ایجاد شده اند.

دید لایه ای

شکل بعد، عناصر تشکیل دهنده ی سامانه ی پرداخت خرد و ارتباطات آنها را نمایش می دهد. در این دید به کار گیری الگوی معماری لایه ای متصور است. در این دید سیستم از ۵ لایه تشکیل شده است.لایه ها به شرح زیر هستند:

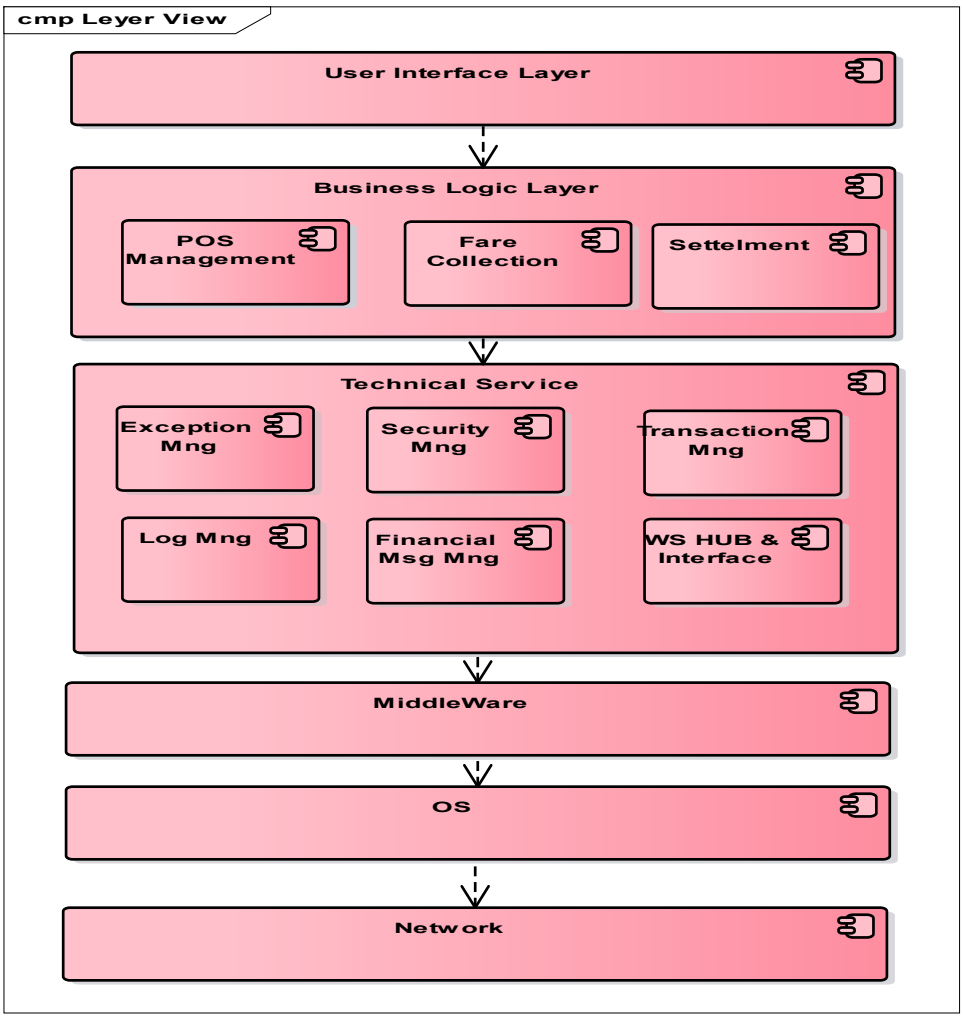
لایه *ی واسط کاربری* مسئول نمایش اطلاعات تراکنش ها و منو های ترمینال و نیز مشمول نمایش صفحات و سناریو های وب تسهیم است.

لایه *منطق* مسئول نیاز های وظیفه مندی است، در واقع این لایه کارکرد مورد انتظار ذی نفعان را نمایش می دهد.

لایه *ی سرویس های تکنیکی* ، کارکرد های مورد نیاز برای سیستم را فراهم می آورد. لایه ی سیستم عامل که سیستم سمت سرور و سمت ترمینال ها روی آن اجرا می شود. در سمت ترمینال ها نوع کوچک شده لینوکس و در سمت سرور از سیستم عامل خانواده ی ویندوز استفاده می شود.

در لایه *ی* شبکه ، تجهیزات سخت افزاری و اتصالات شبکه ای تعریف می شود.

با استفاده از دید لایه ، امنیت و اصلاح پذیری را به ارمغان می آوریم.



شکل ۱- دید لایه

دید استقرار

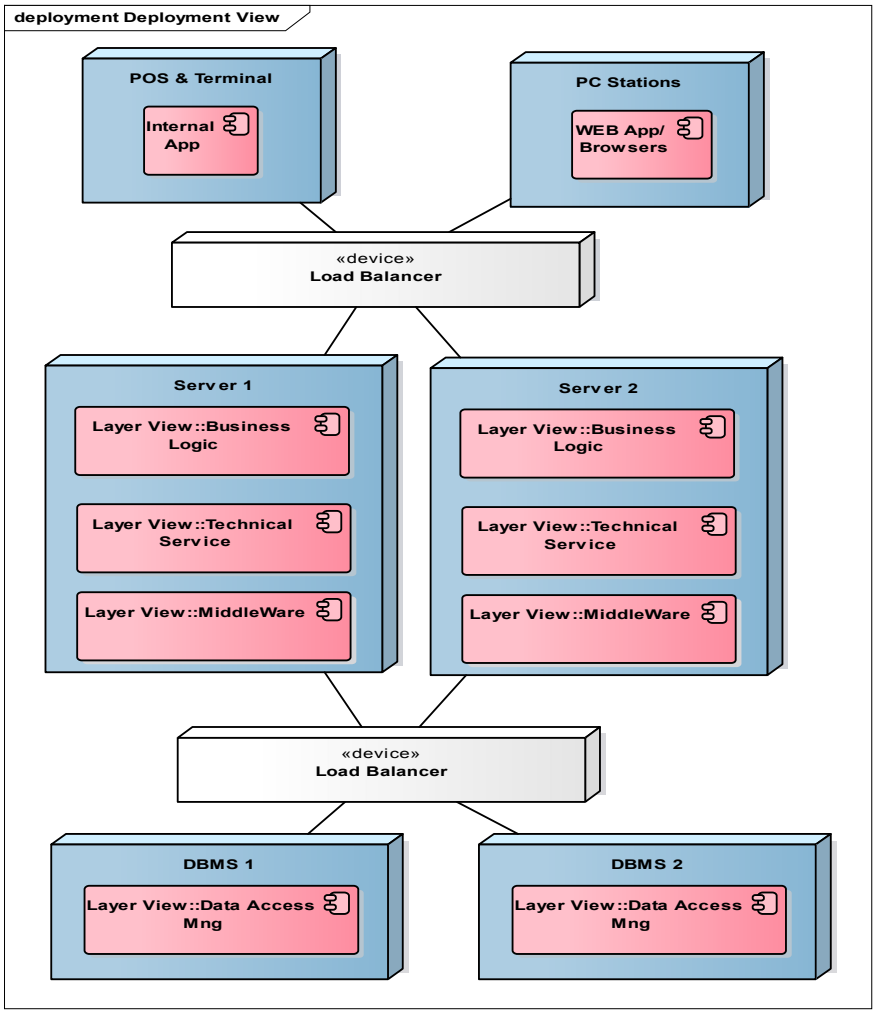
در این دید نحوه توزیع و قرارگیری مولفه های سیستم پرداخت خرد روی ابزار های محاسباتی را نمایش می دهیم. این دید چگونگی تحقق قابلیت دسترسی، کارایی و امنیت را نشان می دهد.

مولفه Load balancer مسئول دریافت درخواست ها از سمت ترمینال ها و کاربران وب تسهیم است. ما در جهت بالا بردن قابلیت دسترسی چند نسخه از منطق برنامه را روی وب سرور ها توزیع می کنیم.

مولفه Load balancer با دریافت درخواست ها آنها را میان وب سرور توزیع می کند. به عبارت بهتر سیستم در سمت سرور به گونه ای طراحی شده است که بر روی مجموعه ای از پردازنده ها کار می کند. این مجموعه پردازنده ها هر یک نسخه ی مجزا از سرویس های سیستم را اجرا می کنند.

در هر وب سرور نیز از تاکتیک نظارت، جهت بررسی مداوم سلامت سیستم استفاده می شود. تعداد وب سرور ها (یا پردازنده ها) به دلیل جلب توافق کارفرما و هزینه های مربوطه هنوز قطعی نشده است و این همان تاثیر معماری بر ویژگی های کیفی حرفه است که بایستی مورد حل و فصل قرار گیرد.

دید استقرار در شکل بعد ، چگونگی افزایش قابلیت دسترس پذیری مولفه ها را با تاکتیک افزونگی فعال نمایش می دهد.



شکل ۲- دید استقرار

دید پیاده سازی(دید کد)

دید کد، چگونگی توزیع وظیفه مندی به واحد های کد را نشان می دهد.

در سیستم پرداخت مد نظر ما، عناصر عملیاتی سیستم به کلاسها و وب سرویس ها نگاشته می شوند. این دید برای تیم توسعه بسیار مفید است. هرچند که این دید چندان به نمایش ویژگی های کیفی نمی پردازد اما برای تیم توسعه بسیار مفید است.

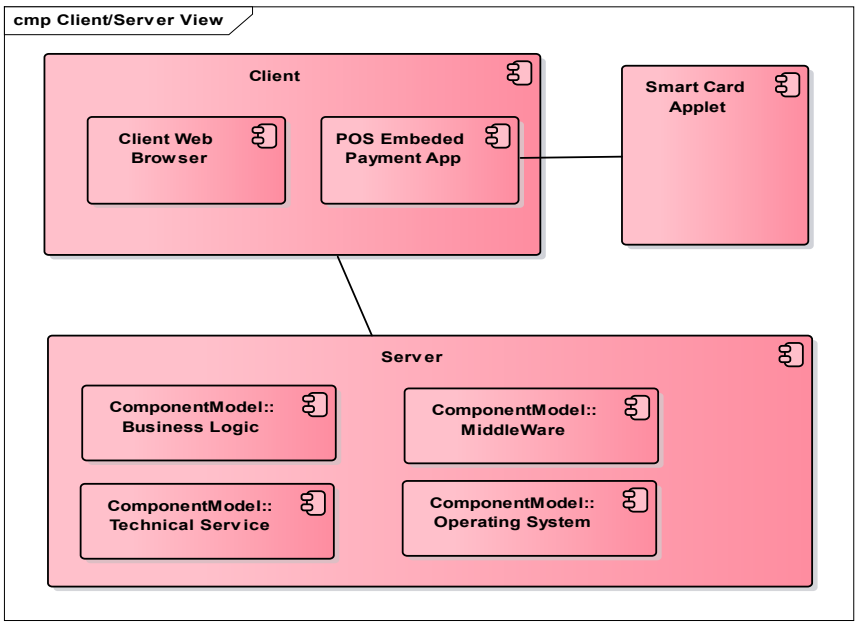
```
User Interface Layer
در لایه واسط کاربری کد زیر اجرا می شود //
{
Terminal.getInstance().doLogin(perfection.creds("172510084")[0], 1));}
//---------------------------------------------------------------------------
در لایه منطق کسب و کار کد زیر اجرا می شود//
اجرای سرویس ها به کمک کلاسها که مسول قواعد سیستم هستند انجام می شوند //
Business Layer
سرویس ورود به سیستم//
package ePurse.Security
   man = Manager.getInstance();
     ready = man.isReadey();

       status = man.getNewElStatus();
     }  }
//---------------------------------------------------------------------------
در لایه دسترسی داده ها نگاشت کلاس ها به داده ها  و بالعکس انجام می شود//
package ePurse.Security.DataAccessComponentFacade
Public GetUserAccess(Credential){
اکنون به کمک الگوی فکتوری کلاس نگاشت کننده را ایجاد می کنیم//
}

PersistantFactory{
Public static class createMapper( Terminal posIns){
  Switch x
    Case 1; ... Case n;
}}
```

دید کلاینت/ سرور

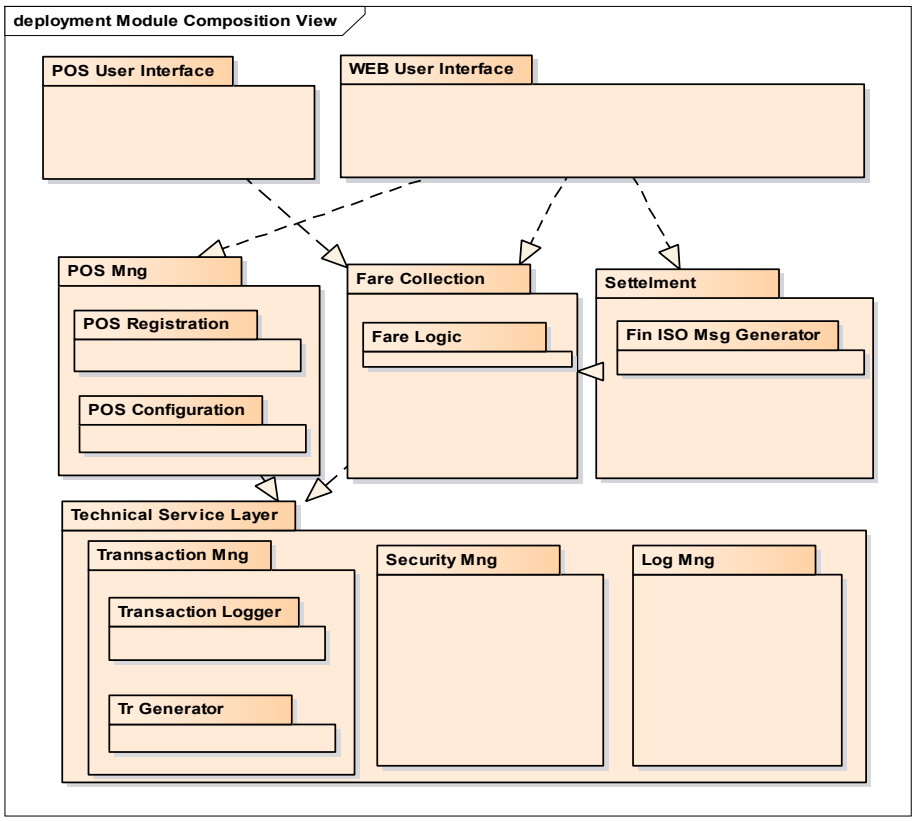
سیستم پرداخت خرد یک سیستم توزیع شده است. از این رو نمایش این دید الزامی است. دید کلاینت/سرور نحوه توزیع مؤلفه های سیستم را بین سرویس دهنده و سرویس گیرنده نشان می دهد. این دید تحقق ویژگی کیفی کارایی و قابلیت نگهداری را نشان می دهد. به این ترتیب که جهت تحقق کارایی بخشی از پردازش ها روی سرویس گیرنده و سرویس دهنده قرار گیرد.



شکل ۳- دید خادم و مخدوم

دید تجزیه ماژول

این دید وظیفه مندی سیستم را نشان می دهد. این دید راهنمای خوبی برای مدیر پروژه جهت طرح ریزی پروژه و تقسیم کار است. این دید قابلیت نگهداری را نشان می دهد.



شکل ۴- دید تجزیه ماژول

به این ترتیب تا این جا ، با مشخص کردن مجموعه ی نیازمندی های وظیفه مندی و غیر وظیفه مندی ، مجموعه ای از تاکتیک ها را اتخاذ کردیم، سپس با دید های مختلف چگونگی تحقق ویژگی های کیفی را نشان دادیم.

نمونه سازی عناصر معماری و تخصیص مسؤلیت به آنها

مسئولیت عناصر تشکیل دهنده ی سیستم به شرح زیر است.

مولفه	مسئولیت
واسط کاربری	این مؤلفه مسئول تعامل با کاربر است. درمورد نرم افزار ترمینال های واسط کاربری شامل منوهای خرید شارژ و تنظیمات دستگاه است و پیغام های تعاملی با کاربران (صاحب فروشگاه و دارنده کارت) از طریق این واسط رد و بدل می شوند. در مورد وب تسهیم نیز ، صفحات وب که در وب سرور موجود اند و بنا به درخواست کاربران در بروز ها بارگذاری می شوند نیز مصادیق واسط کاربری این سیستم هستند.
مدیریت پوزها و ترمینال ها	این مؤلفه مسئول مدیریت شناسایی و ثبت POS ها و ترمینال های متصل به سامانه است.
مدیریت امنیت	این مؤلفه مسئول فراهم کردن روش های حفظ امنیت سیستم است این مؤلفه با دریافت درخواست های رسیده از سمت کاربران و ترمینال ها، مجاز بودن آنها را بررسی می کند.
مدیریت تراکنش ها	این مؤلفه مسئول تولید تراکنش های خرید شارژ و بررسی نتایج آنها است.
مدیریت خطا	این مؤلفه مسئول کشف خطاهای رخ داده در سیستم در هنگام اجرا است.
مدیریت دسترسی داده ها	این مؤلفه مسئول کنترل دسترسی سایر مؤلفه های سیستم به منابع داده ی سیستم است.
مؤلفه مدیریت کارتخوان	این مؤلفه مسئول مدیریت وضعیت کارتخوان غیر تماسی به عنوان قلب ترمینال ها برای

	انجام تراکنش با کارت ها است.

تعریف واسط هایی که عناصر ارائه می دهند

تعریف رابط های مؤلفه ها در واقع مسؤلیت های مورد انتظار از مؤلفه های سیستم را نمایش می دهند. بنابر این لازم است مسؤلیت های هر مؤلفه از سیستم تعریف و مستند سازی شود. ما در اینجا رابط مؤلفه های سیستم را به طور مختصر تعریف و مستند سازی میکنیم.

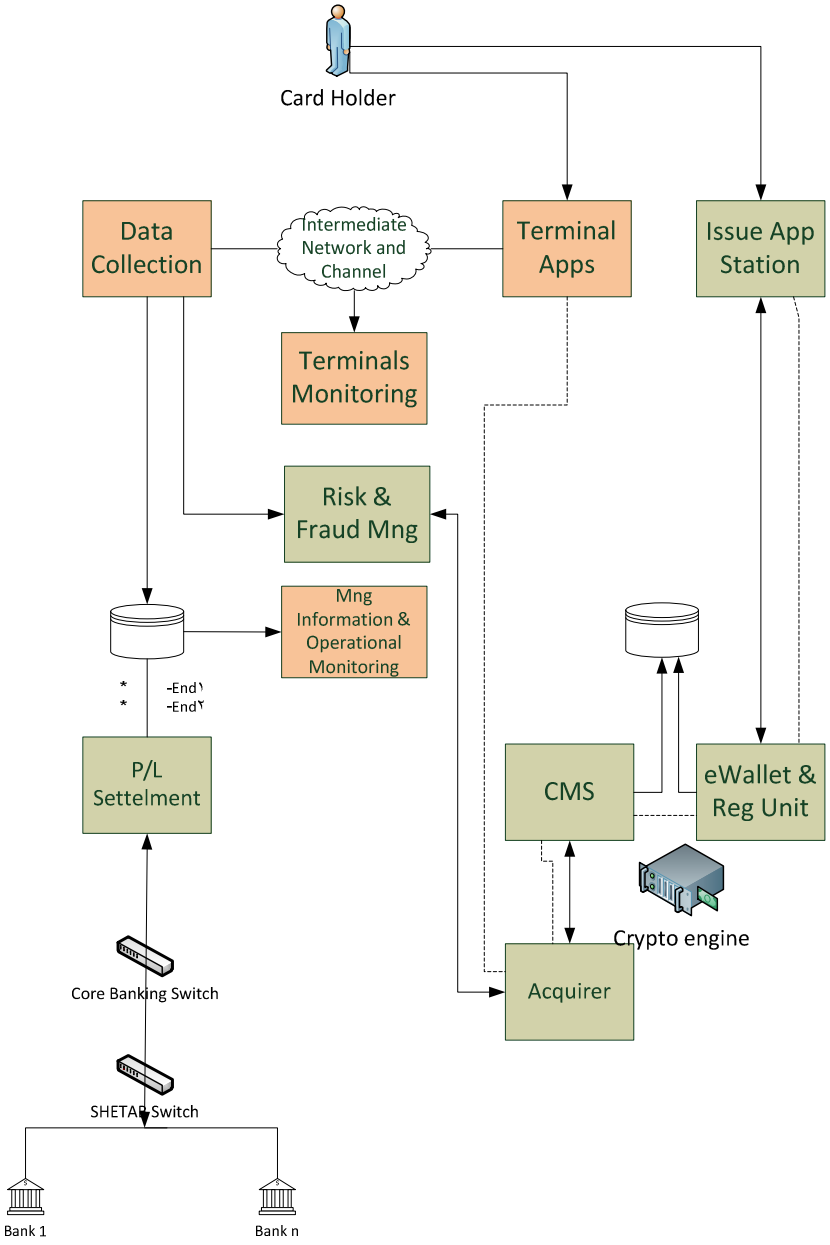
از عنصر	به عنصر (فراهم می کند برای)	واسط ارایه شده
واسط کاربری	کاربر	تمام کارکرد های مورد انتظار از سیستم
مدیریت پوزها و ترمینال ها	واسط کاربر	ثبت ترمینال جدید- تعریف ذی نفعان – تعریف کارمزد ذی نفعان
مدیریت امنیت	تمام مؤلفه ها	اعتبار سنجی - احراز هویت- بررسی مجاز بودن عمل
مدیریت تراکنش ها	واسط کاربر	ارتباط برقرار کردن منوهای برنامه ریزی تولید تراکنش بنابر نوع منوی انتخابی- بررسی پاسخ دریافتی به ازای تراکنش ها
مدیریت خطا	تمام مولفه ها	دریافت خطا و ذخیره ی آن- نمایش فرم هشدار خطا به کاربر
مدیریت دسترسی داده ها	مدیریت تراکنش و مدیریت امنیت	صفحه ی ورود به وب تسهیم

بررسی درستی مراحل

در این مرحله به بررسی و ارزیابی مراحل طی شده می پردازیم تا چیزی فراموش نشده باشد.

در تکرار دوم از فرایند ADD یکی دیگر از مؤلفه ها انتخاب می شود و همه مراحل قبلی روی آن تکرار می شود. بنابراین تکرار های بعدی مشابه تکرار اول است . تکرار ها آنقدر ادامه می یابد تا طراحی تمام عناصر به کمک ADD صورت گیرد.

نهایتا نمای بالای مولفه های سامانه و ارتباطات آنها در شکل زیر به تصویر کشیده شده است:



شکل ۵- نمای بالای سیستم