بسم الله الرحمن الرحیم

راه‌کارهای امن‌سازی سیستم‌های اطلاعاتی

دانشگاه‌ها و مراکز آموزشی

شرکت مهندسی پیام‌پرداز

آذر ماه ۸۹

این پیشنهاد توسط شرکت پیام‌پرداز تهیه شده است و هرگونه استفاده از تمام یا بخشی از آن منوط به اجازه کتبی از این شرکت می‌باشد.

فهرست

عنوان **صفحه**

۱- مقدمه ۱
۲- سیستم آموزش ۲
۲-۱- نیازمندی‌های امنیتی ۲
۲-۲- راه حل‌های امن‌سازی ٤
۲-۲-۱- راه حل مبتنی بر مکانیزم *SSL* ٤
۲-۲-۲- راه حل مبتنی بر محصول کیهان ۷
۳- دانشگاه مجازی ۹
۳-۱- نیازمندی‌های امنیتی ۹
۳-۲- راه حل امن‌سازی ۹
۴- اتوماسیون اداری ۱۰
۴-۱- نیازمندی‌های امنیتی ۱۰
۴-۲- راه حل امن‌سازی ۱۱

۱- مقدمه

رشد و گسترش روزافزون فناوری اطلاعات، انقلابی را در ابعاد مختلف زندگی انسانها و عملکرد سازمانها ایجاد کرده است. این فناوری روشهای کارکرد و نگرش افراد، سازمانها و دولتها را دگرگون ساخته و باعث ایجاد صنایع نوین، مشاغل جدید و خلاقیت در انجام امور شده است. ظهور پدیده‌هایی همچون آموزش مجازی و آموزش از راه دور از نتایج عمده نفوذ و گسترش فناوری اطلاعات در عرصه آموزش است.

سرویس‌های مهم الکترونیکی در یک دانشگاه نوعی عبارتند از:

- آموزش
- دانشگاه مجازی
- اتوماسیون اداری

با توجه به رشد سریع حملات الکترونیکی همگام با رشد تکنولوژی و حرفه‌ای شدن مجرمین فضای *Cyber*، امن‌سازی سرویس‌های الکترونیکی یکی از مسائل مهم پیش رو و از دغدغه‌های عمده مدیران *IT* دانشگاه‌ها و مراکز آموزشی است.

هدف از این نوشتار مروری سریع بر تهدیدات امنیتی پیش رو در سیستم اطلاعاتی دانشگاه‌ها و ارایه راه‌کارهایی برای امن‌سازی آن می‌باشد. راه‌کارهای ارایه شده جنبه عمومی داشته و در آنها شرایط ویژه فنی و مسایل خاص موجود در دانشگاه‌های مختلف لحاظ نشده است. لذا در صورت لزوم باید با

توجه به شرایط شبکه دانشگاه مورد نظر، طراحی‌های خاص منظوره و یا بومی‌سازی‌هایی در محصولات ارایه شده انجام گیرد.

شرکت مهندسی پیام‌پرداز بر این باور است که براساس توان، تجربه و سوابق کارهای انجام شده، قابلیتهای لازم را برای طراحی معماری امنیت سیستم اطلاعاتی دانشگاه‌ها و اجرای امن‌سازی آن داراست. این قابلیتها منبعث از دانش و تجربه عملی کارشناسان شرکت در زمینه ارایه خدمات مشاوره و اجرای امنیت فضای تبادل اطلاعات و به ویژه برخورداری از یک سبد متنوع از محصولات امنیت فناوری اطلاعات در این شرکت می‌باشد.

در ادامه به معرفی راه‌کارهای امن‌سازی سرویس‌های مختلف در یک دانشگاه نوعی می‌پردازیم.

۲- سیستم آموزش

منظور از سیستم آموزش یک برنامه کاربردی تحت وب و یا یک برنامه کاربردی *Desktop* است که معمولا از طریق اینترنت و یا اینترانت به وسیله اساتید، دانشجویان و کارمندان مورد استفاده قرار می‌گیرد و خدمات آموزشی را به طور متمرکز در اختیار کاربران قرار می‌دهد. این سیستم دارای حیطه‌بندی بوده و پس از احراز اصالت کاربر در بدو امر، دسترسی‌های مجاز را کنترل می‌نماید. به عنوان مثال اساتید معمولا برای وارد کردن نمرات درسی، لیست حضور و غیاب و کار با نظام ارزشیابی اساتید با این سیستم کار می‌کنند. دانشجویان از این سیستم برای ثبت نام دروس، دیدن نمرات و کارنامه و انجام امور اداری نظیر صدور اشتغال به تحصیل و کارمندان برای بررسی وضعیت دانشجویان یا اساتید، برنامه‌ریزی زمان ارایه دروس و گزارش‌گیری‌های مختلف استفاده می‌نمایند.

۲-۱- نیازمندی‌های امنیتی

از آنجا که عملیات انجام گرفته با سیستم آموزش معمولا حساس هستند این سیستم به سرویس‌های مختلف امنیتی از قبیل موارد زیر نیاز دارد:

- احراز اصالت[1] کاربر برای سرور: لازم است هویت کاربر در هنگام درخواست سرویس به صورت کاملا مطمئن برای سرور احراز گردد تا بتوان امکانات لازم را در اختیار وی قرار داد. روش معمول در این حالت استفاده از نام و کلمه عبور است که دارای ضعف‌های زیادی است. به عنوان مثال انتخاب کلمات عبور ضعیف توسط کاربران، شنود کلمه عبور از روی شبکه، سرقت کلمه عبور با استفاده از برنامه‌های *Key Logger* از روی کامپیوتر کاربر و حمله

[1] *Authentication*

دیکشنری نمونه‌ای از تهدیدات روش احراز اصالت یک عاملی است. برای رفع این مشکلات روش‌های احراز اصالت دوعاملی[1] پیشنهاد می‌شود که در آن علاوه بر کلمه عبور (یا اصطلاحا *PIN*[2]) از یک توکن امنیتی[3] نیز برای بررسی هویت کاربر استفاده می‌شود.

- احراز اصالت سرور برای کاربر: کاربر نیز لازم است از اصالت سروری که بدان متصل شده اطمینان حاصل کند. در واقع ممکن است کاربر با یک سرویس‌دهنده جعلی (در یک حمله *Phishing*) ارتباط برقرار کند و اطلاعات خود را برای سرویس‌دهنده جعلی فاش نماید.
- کنترل دسترسی: پس از احراز اصالت کاربر لازم است سطح دسترسی وی به منابع بررسی و کنترل گردد. به عنوان مثال کاربر بسته به اینکه عضو گروه اساتید، دانشجویان و یا کارمندان است وظایف و مسئولیت‌های متفاوتی دارد و بنابراین اجازه دسترسی به برخی امکانات سیستم به وی داده می‌شود. همچنین علاوه بر گروه کاربر، هر کاربر نیز به طور خاص دسترسی‌های محدودی خواهد داشت.
- ردگیری[4] فعالیت‌های کاربر: به منظور پیش‌گیری از وقوع اقدامات خلاف توسط کاربران و نیز تشخیص و ردگیری این‌گونه فعالیت‌ها در صورت وقوع، سیستم‌های اطلاعاتی کلیه فعالیت‌های انجام گرفته را رویدادنگاری کرده و آنها را در اختیار مدیر سیستم قرار می‌دهند. بسته به سطح رویدادنگاری و جزییات مورد نظر، ممکن است عملیات ردگیری توسط برنامه‌های کاربردی و یا تجهیزات شبکه انجام بگیرد.
- محرمانگی[5] داده‌های مبادله شده: محرمانگی اطلاعات حساس مبادله شده بین کامپیوتر کاربر و سرور باید با روش‌های مدرن رمزنگاری تامین گردد تا هیچ‌کس امکان شنود اطلاعات را از روی شبکه نداشته باشد. به عنوان مثال ممکن است فرد نفوذی کلمه عبور یک کاربر را بر روی شبکه شنود کرده و با ایفای نقش به منابع و اختیارات وی دسترسی پیدا کند.
- صحت[6] داده‌های مبادله شده: از آنجا که اعتبار داده‌های آموزشی (همچون نمرات) از حساسیت زیادی برخوردار است لذا باید با بکارگیری روش‌های مناسب، صحت اطلاعات مبادله شده بین کامپیوتر کاربر و سرور را بر روی شبکه تضمین کرد.
- جلوگیری از نفوذ به *LAN* مرکزی: از آنجا که معمولا شبکه مرکزی دانشگاه (حاوی سرورهای

---

[1] *Two-Factor*
[2] *Personal Identity Number*
[3] *Secure Token*
[4] *Auditing*
[5] *Confidentiality*
[6] *Integrity*

اصلی و پایگاه‌های داده) به شبکه‌های عمومی نظیر اینترنت متصل است امکان نفوذ هکرها به شبکه مرکزی دانشگاه و انجام فعالیت‌های خراب‌کارانه از قبیل تغییر اطلاعات پایگاه‌های داده و حملات ازکاراندازی سرویس[1] (*DoS*) وجود دارد. بنابراین لازم است با استفاده از دیواره‌های آتش[2] مناسب از نفوذ بسته‌های بیگانه به شبکه داخلی جلوگیری کرد.

۲-۲- راه حل‌های امن‌سازی

راه حل‌های امن‌سازی برای سیستم آموزش را می‌توان به دو دسته راه حل مبتنی بر مکانیزم *SSL* و راه حل مبتنی بر سیستم کیهان تقسیم‌بندی کرد.

۲-۲-۱- راه حل مبتنی بر مکانیزم *SSL*

برای برطرف کردن تهدیدات موجود، نیاز به استفاده از مکانیزم‌های امنیتی برای امن‌سازی ارتباط بین *Client* و سرور است. یک راه حل مرسوم در این زمینه، خصوصا در صورتی که سیستم آموزش مبتنی بر وب باشد استفاده از پروتکل استاندارد *SSL*[3] است. این پروتکل در مرورگرهای مختلف پشتیبانی شده و بدون دغدغه می‌توان از آن استفاده نمود. در این پروتکل پس از طی مرحله احراز اصالت طرفین با استفاده از گواهی دیجیتال[4]، یک کلید جلسه توافق شده و پس از آن اطلاعات به صورت امن مبادله می‌گردد.

با توجه به سطح امنیت مورد نیاز، *SSL* را می‌توان به دو صورت به کار گرفت. در ادامه به نحوه بکارگیری این دو روش و محاسن و معایب هر یک می‌پردازیم.

الف- استفاده از *SSL* با احراز اصالت دوطرفه

در این روش *Client* و سرور هر دو دارای گواهی دیجیتال هستند و با استفاده از آن اصالت خود را به طرف مقابل اثبات می‌کنند. گواهی هر طرف در این حالت حاوی کلید خصوصی، کلید عمومی و امضای مرکز صدور گواهی[5] (*CA*) بر روی پارامترهای عمومی گواهی است. در این روش سرویس‌های امنیتی احراز اصالت طرفین، محرمانگی داده‌ها و صحت داده‌ها به طور کامل ارایه می‌گردد. از این تکنیک می‌توان برای امن‌سازی ارتباط اساتید و کارمندان با سیستم آموزش که از

---

[1] *Denial of Service*
[2] *Firewall*
[3] *Secure Socket Layer*
[4] *Certificate*
[5] *Certificate Authority*

اهمیت بیشتری برخوردار است استفاده جست. البته با توجه به این که مکانیزم *SSL* در لایه انتقال[1] انجام می‌پذیرد در این حالت فرایند احراز اصالت باید در برنامه کاربردی تحت وب نیز انجام گردد. به همین منظور پس از برقراری کانال امن *SSL*، نام و کلمه عبور کاربر در صفحه وب پرسیده شده و برای سرویس‌دهنده ارسال می‌گردد (البته امکان دریافت اطلاعات گواهی کاربر در محیط *ASP.NET* بر روی وب سرور *IIS* و ارایه سرویس *SSO* وجود دارد).

یکی از چالش‌های اصلی این روش، نحوه نگهداری امن گواهی کاربران است. معمولا کاربران گواهی را بر روی هارد کامپیوتر خود ذخیره می‌کنند. بنابراین امکان جابجایی کاربر و استفاده از کامپیوترهای دیگر به راحتی میسر نیست. از طرف دیگر از آنجا که این گواهی حاوی کلید خصوصی کاربر است در صورتی که به دست افراد سودجو بیافتد می‌توانند از آن سوء استفاده کرده و خود را به جای کاربر به سرور معرفی نمایند. برای رفع این مشکل به جای نصب گواهی در کامپیوتر کاربر از توکن‌های امنیتی برای ذخیره امن گواهی استفاده می‌شود. در این صورت کلید خصوصی کاربر در مکان امنی قرار گرفته و امکان دسترسی غیر مجاز به آن وجود نخواهد داشت. توکن‌های امنیتی معمولا به دو صورت کارت هوشمند و ماژول *USB* هستند که انواع مختلفی از آنها در بازار وجود دارد. یکی از اشکالات اصلی کارت هوشمند این است که برای کار با آن نیاز به یک دستگاه کارت‌خوان وجود دارد که ممکن است در خیلی از مکان‌ها در دسترس نباشد. لذا امروزه در کاربریهای متداول کامپیوتری، توکن‌ها امنیتی مبتنی بر پورت *USB* به دلیل سهولت استفاده از استقبال بیشتری برخوردار شده‌اند.

یک انتخاب مناسب برای توکن امنیتی ماژول سخت‌افزاری کیاست. این توکن امنیتی که از نوع *USB* است و از ویژگی‌های ممتاز امنیتی برخوردار می‌باشد برای اولین بار در کشور در سال ۱۳۸۳ به وسیله شرکت پیام‌پرداز ارایه گردید. مراحل طراحی، توسعه و تولید این محصول به صورت کامل در داخل شرکت پیام‌پرداز و زیر نظر تیم‌هایی متشکل از متخصصین امنیت، سخت‌افزار و نرم‌افزار انجام گرفته است. توکن سخت‌افزاری کیا با پشتیبانی از استانداردهای *PKCS#11* و *CSP*، در مرورگرهای مختلف از قبیل *IE* و *Firefox* (و دیگر کاربردهای استاندارد مبتنی بر *PKI*) به عنوان محل ذخیره‌ی گواهی‌های کاربران قابل بکارگیری است.

ب- استفاده از *SLL* با احراز اصالت یک‌طرفه

در *SSL* احراز اصالت *Client* اختیاری است و می‌توان در پروتکل *SSL* از آن صرف نظر نمود. در

[1] *Transport Layer*

این حالت فقط نیاز به گواهی سرویس‌دهنده است و کاربران نیازی به داشتن گواهی برای برقراری ارتباط نمی‌باشند. واضح است که در این وضعیت سرویس‌دهنده برای کاربران احراز اصالت می‌شود اما کاربر برای سرویس‌دهنده احراز اصالت نمی‌گردد.

این روش به خاطر سادگی استفاده، بسیار مرسوم بوده و در اکثر سرویس‌دهنده‌های وب خصوصا در صفحه‌های ورود اطلاعات حساس (مثل نام و کلمه عبور یا اطلاعات کارت‌های اعتباری) مورد استفاده قرار می‌گیرد. از این تکنیک می‌توان برای امن‌سازی ارتباط دانشجویان با سیستم آموزش استفاده نمود. با توجه به این که در این حالت نیز احراز اصالت کاربر مورد نیاز است، فرایند احراز اصالت باید در برنامه کاربردی تحت وب انجام گیرد. به همین منظور پس از برقراری کانال امن *SSL*، نام و کلمه عبور کاربر در صفحه وب پرسیده می‌شود.

اگرچه با ایجاد شدن کانال *SSL* (در هر یک از دو روش فوق) سرویس‌های محرمانگی و صحت داده‌ها محقق می‌شود و بخش مهمی از حملات مرتفع می‌گردد اما هنوز استفاده نادرست و بدون آگاهی از *SSL* می‌تواند زمینه حملات مهم دیگری از جمله *Man in the Middle* را فراهم نماید. این حمله زمانی می‌تواند بروز نماید که سرویس‌دهنده از گواهی معتبری استفاده نکند و یا اینکه گواهی *CA* مربوط به سرویس‌دهنده بر روی کامپیوتر کاربر وجود نداشته باشد. در هر دو حالت اخطاری مبنی بر نامعتبر بودن گواهی سرویس‌دهنده به کاربر گزارش داده می‌شود که چون معمولا کاربران با مسائل امنیتی آشنایی کافی ندارند هشدار سیستم را نادیده گرفته و ارتباط *SSL* با سرویس‌دهنده مزبور را (بدون اطمینان از واقعی یا جعلی بودن آن) قبول می‌نمایند. افراد سوء استفاده کننده می‌توانند از این سهل‌انگاری کاربر استفاده کرده و سرور جعلی خود را به جای سرور اصلی معرفی نموده و کانال *SSL* را با کاربر برقرار کنند. بدین ترتیب کاربر اطلاعات محرمانه خود (از قبیل نام و کلمه عبور) را در اختیار سرور جعلی قرار داده و سرور جعلی به جای کاربر با سرور اصلی ارتباط برقرار می‌کند و پاسخ‌های سرور را برای کاربر برمی‌گرداند (حمله *Man in the Middle*). بنابراین کاربر از وقوع حمله مطلع نخواهد شد. در این حمله کافی است حمله کننده یکبار این عملیات را انجام داده و با بدست آوردن نام و کلمه عبور، سوء استفاده‌های بعدی را به راحتی انجام دهد.

برای رفع مشکل فوق به دو صورت می‌توان عمل کرد:

- تهیه گواهی از CAهای بین‌المللی که کامپیوتر کاربر به طور خودکار اعتبار آن را تشخیص می‌دهد:

در موقع نصب سیستم عامل ویندوز مجموعه‌ای از گواهی *CA*های مهم از جمله *VeriSign*،

Thawate و ... به طور خودکار بر روی کامپیوتر کاربر نصب می‌شود. بنابراین اگر گواهی سرور وب توسط این مراجع امضا شده باشد کامپیوتر کاربر به طور خودکار گواهی سرور را معتبر و قابل قبول تلقی می‌کند.

- تهیه گواهی از CAهایی که نیاز به نصب گواهی دارد:

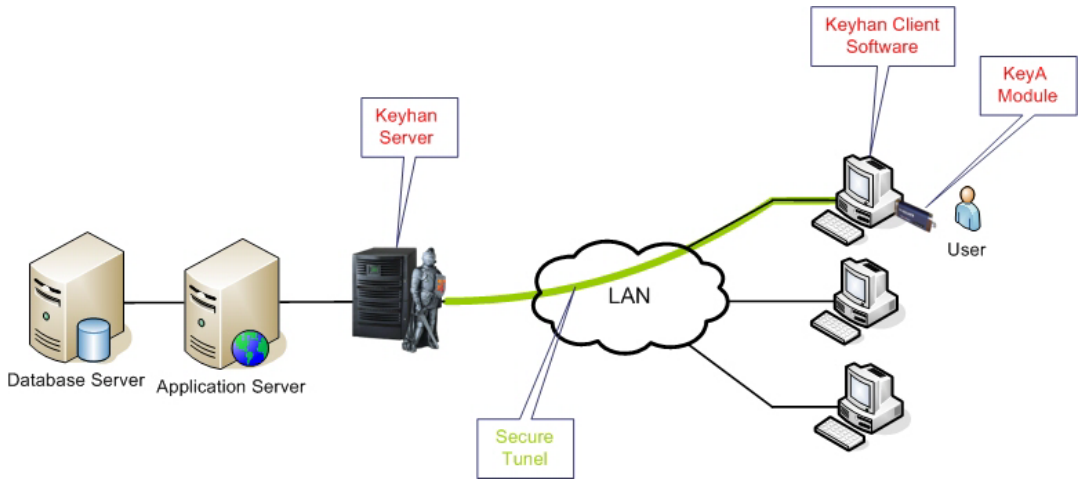
در این روش برای تشخیص صحت گواهی سرور وب، نیاز به نصب گواهی *CA* صادر کننده در کامپیوتر می‌باشد. در این حالت کاربر باید با مراجعه به صادر کننده گواهی و تشخیص معتبر بودن آن، گواهی مربوطه را در لیست گواهی‌های معتبر[1] کامپیوتر خود نصب کند. پس از نصب گواهی *CA*، در ارتباطات بعدی گواهی ارسالی از طرف سرویس‌دهنده معتبر تلقی می‌شود. روشن است که در این حالت آگاهی دادن به کاربران مساله بسیار مهمی است. برای صدور گواهی کاربران، دانشگاه می‌تواند یک مرکز *CA* با گواهی خودامضا[2] راه‌اندازی کرده و برای کاربران گواهی صادر نموده و به آنان تحویل داده و یا در توکن امنیتی آنان تزریق کند.

۲-۲-۲- راه حل مبتنی بر محصول کیهان

در صورتی که سطح بالاتری از امنیت برای ارتباط کاربران با سرور مد نظر باشد (اعم از برنامه‌های تحت وب یا *Desktop*) می‌توان از سیستم امن‌سازی کیهان بدین منظور استفاده کرد. این محصول توسط شرکت پیام‌پرداز طراحی و پیاده‌سازی شده است.

شکل ۱ طرح امن‌سازی سیستم آموزش را با محصول کیهان نشان می‌دهد. در این طرح یک سرویس‌دهنده کیهان در جلوی سرور وب قرار گرفته و بر روی هر یک از کامپیوترهای کاربران نرم‌افزار *Client* کیهان نصب می‌شود. هر کاربر برای ارتباط با سرور وب ابتدا لازم است از طریق سرور کیهان احراز اصالت شده و اجازه دسترسی وی صادر گردد. فرایند احراز اصالت کاربر با استفاده از یک پروتکل احراز اصالت اختصاصی و به صورت دوعاملی (با بکارگیری ماژول کیای کاربر و *PIN* وی) انجام می‌گیرد. پس از احراز اصالت موفقیت‌آمیز کاربر، یک تونل امن بین کامپیوتر کاربر و سرور کیهان برقرار می‌شود که کلیه داده‌های مبادله شده درون آن رمز می‌شود و بدین ترتیب سرویس‌های محرمانگی و صحت تامین می‌گردد.

[1] *Trusted Root Certificate Authority*
[2] *Self-Sign*



شکل ۱: امن‌سازی سیستم آموزش با محصول کیهان

سیستم کیهان در لایه شبکه عمل کرده و از دید لایه کاربرد کاملا شفاف است. بنابراین نیازی به تغییر در برنامه کاربردی وب فعلی وجود نخواهد داشت. از طرف دیگر سرویس خاصی که محصول کیهان می‌تواند ارایه کند سرویس اختصاص آدرس *IP* مجازی به کاربر است که با استفاده از آن می‌توان با تغییرات جزیی در برنامه کاربردی وب فعلی، سرویس ورود یک‌باره[1] (*SSO*) را در شبکه ارایه نمود. بدین ترتیب کاربر با یک بار *Login* به سیستم کیهان احراز اصالت می‌شود و برنامه کاربردی جهت احراز اصالت، نیازی به گرفتن نام و کلمه عبور کاربر ندارد.

در صورتی که به دلیل بالا رفتن هزینه، امکان ارایه ماژول کیا به همه کاربران نباشد می‌توان با توجه به حساسیت بیشتر ارتباط اساتید و کارمندان با سرور آموزش، ماژول‌های کیا را تنها در اختیار این گروه از کاربران قرار داد و سیستم کیهان را به گونه‌ای تنظیم کرد که ارتباط اساتید و کارمندان با سرور آموزش، تحت حفاظت سیستم کیهان و ارتباط دانشجویان با سرور آموزش، بدون حفاظت کیهان و با همان روش معمول انجام پذیرد. در این حالت باید تغییرات جزیی در برنامه کاربردی ایجاد گردد.

سرویس‌های امنیتی ارایه شده در این طرح عبارتند از: احراز اصالت دوعاملی کاربر، احراز اصالت سرور، کنترل دسترسی کاربر، محرمانگی و صحت داده‌های مبادله شده، جلوگیری از نفوذ به سرورها، ردگیری فعالیت‌های کاربر در سطح شبکه (شامل زمان‌های ورود و خروج و ...) و امکان ارایه سرویس *SSO*.

[1] *Single Sign On*

۳- دانشگاه مجازی

امروزه خدمات دانشگاه مجازی یا *e-Learning* گسترش زیادی در مراکز آموزشی دنیا یافته است و روز به روز بر حجم این خدمات و تنوع مکانیزم‌های آن افزوده می‌شود. در این سیستم دانشجو و استاد از طریق شبکه اینترنت به صورت غیر حضوری در کلاس درس مجازی حاضر شده و به آموزش و فراگیری دانش می‌پردازند.

۳-۱- نیازمندی‌های امنیتی

سرویس‌های امنیتی مورد نیاز در یک سیستم دانشگاه مجازی مواردی از قبیل زیر هستند:

- احراز اصالت دانشجو: برای ارایه خدمات آموزش از راه دور لازم است ابتدا هویت کاربر برای سرور احراز گردد.
- کنترل دسترسی: از آنجا که در سیستم دانشگاه مجازی رشته‌های مختلف آموزشی وجود دارد لازم است سطح دسترسی کاربر به منابع درسی کنترل گردد. به عنوان مثال دانشجوی هر رشته تنها باید اجازه دسترسی به منابع آموزشی همان رشته را داشته باشد.
- جلوگیری از تکثیر غیر مجاز محتواهای آموزشی: مطالب و محتواهای آموزشی معمولا از نظر مراکز آموزشی ارزش زیادی دارند ولیکن به دلیل ماهیت الکترونیکی این مطالب، تکثیر غیر مجاز آنها به راحتی انجام گرفته و حقوق مالکیت معنوی تضییع می‌شود. بنابراین باید با استفاده از تکنیک‌های مناسب از تکثیر غیر مجاز این اطلاعات جلوگیری نمود.

۳-۲- راه حل امن‌سازی

برای امن‌سازی سیستم دانشگاه مجازی نیز می‌توان از سیستم کیهان استفاده نمود. در این حالت سرور کیهان در مقابل سرور دانشگاه مجازی قرار گرفته و بر روی کامپیوتر دانشجو نرم‌افزار *Client* کیهان نصب می‌شود. مدیر سیستم در بدو امر برای هر دانشجو یک ماژول کیا برنامه‌ریزی کرده و در اختیار وی قرار می‌دهد. در این حالت سیستم کیهان ابتدا به صورت قوی (دوسویه و دوعاملی) دانشجو را احراز اصالت کرده و یک تونل امن با کامپیوتر وی برقرار می‌کند. بنابراین سرویس‌های امنیتی احراز اصالت دانشجو و کنترل دسترسی به راحتی قابل ارایه خواهد بود.

نکته مهم قابل توجه این است که با اختصاص ماژول کیا به هر دانشجو می‌توان از قابلیت خاص ماژول کیا در قفل‌گذاری استفاده کرده و سرویس امنیتی جلوگیری از تکثیر غیر مجاز محتواهای آموزشی را نیز به راحتی ارایه نمود. در واقع در صورتی که محتواهای آموزشی از فرمت‌های خاصی پیروی نمایند