# ارایه راهکاری برای افزایش امنیت در وب‌سایت‌ها با استفاده از محدود و مخفی کردن اطلاعات

جعفر عالی‌نژاد[1] – یاسر موحدفرد[2] – محرم کمال[3]
[1] گروه کامپیوتر - دانشگاه آزاد اسلامی واحد پارس آباد مغان
Jprograming_2005@yahoo.com
[2] دانشجوی کارشناسی‌ارشد مهندسی فناوری‌اطلاعات - دانشگاه آزاد اسلامی واحد قزوین
y.movahed@yahoo.com
[3] دانش‌آموخته کارشناسی مهندسی تکنولوژی نرم‌افزار کامپیوتر – دانشگاه علمی کاربردی اردبیل
info@nsa-pm.ir

## چکیده

**امنیت در وب‌سایت، امروزه یکی از چالش‌های اساسی مدیران شبکه است و همواره وب‌سایت‌ها در معرض انواع حملات جدید و ناشناخته هستند. اطلاعات موجود در وب‌سایت‌ها باید از دستیابی غیرمجاز افرادی که نفوذگر نامیده می‌شوند و مجوز دستیابی به داده‌ها را ندارند، محافظت شود. یکی از راهکارهای امنیتی در وب‌سایت‌ها، استفاده از مکانیزم احراز هویت است که این مکانیزم در وب‌سایت‌ها دسترسی کاربران را مدیریت و کنترل می‌کند اما نفوذگر، ممکن است با حمله تغییر پیام، هویت اصلی خود را جعل کرده و به صورت غیر مجاز با ورود به وب‌سایت به اطلاعات دستیابی داشته باشد.**

**در این مقاله پیشنهاد شده است در پایگاه داده، اطلاعات مدیر به صورت کد شده، ذخیره شود و نیز در بخش ورود به سیستم آن رمز را وارد نمود تا منوی فرم مدیریت فعال شود و با کلیک بر روی آن به سرور دیگر که بخش مدیریت فایلها در آن قرار دارد انتقال داده می‌شود، بدین صورت که در فرم مدیریت باز هم سؤال امنیتی و احراز هویت در لایه‌های مختلف داده خواهد شد که تنها در صورت درست بودن همه موارد، امکان دستیابی به برنامه‌ها با توجه به مجوزهای تعریف شده، فراهم می‌شود که موجب دسترسی‌پذیری کابران و مدیران تأیید شده و ایجاد امنیت بالاتر در وب‌سایت‌ها خواهد شد.**

**کلمات کلیدی: امنیت، نفوذگر، تغییر پیام، احراز هویت لایه‌ای**

## ۱- مقدمه

وب‌سایت، مجموعه‌ای از صفحه‌های مرتبط به یکدیگر است که انبوهی از اطلاعات را در قالب متن، تصویر، صدا و فیلم در اختیار بیننده قرار می‌دهد. طراحی یک وب‌سایت افزون بر ایجاد ارتباط و معرفی دارنده سایت، امکان اطلاع‌رسانی به‌روز، بازاریابی و معرفی بین‌المللی را نیز می‌تواند فراهم آورد. وب‌سایت می‌تواند برای عرضه محصول‌ها و خدمات تجاری و هم‌چنین نمونه کار یا معرفی شخص خاص یا حتی ارایه نوشته‌ها و تحقیق‌ها و یا مقاله‌ها به کار رود.

بنابراین می‌توان برای کاربران سطح‌های دسترسی گوناگون تعیین کرد. انواع سطح دسترسی‌ها می‌تواند کاربران ثبت نام شده، کاربران میهمان و سطح مدیران سایت باشد.

کاربران در ابتدای ورود به سایت، اعتبارسنجی می‌شوند و پس از ورود به سایت جهت دسترسی به بخش‌های مختلف با توجه به سطح دسترسی که دارند، هدایت می‌شوند. تدابیر اتخاذ شده در طراحی سایت برای جلوگیری از هر گونه دسترسی غیر مجاز که ممکن است منجر به دستکاری، خرابکاری یا سرقت اطلاعات شود در سه دسته قرار می‌گیرند: تدابیری جهت جلوگیری از ورود خرابکاران به بانک‌های اطلاعاتی و پنل‌های مدیریتی و تلاش برای به دست آوردن کلمه رمز (همه کلمه‌های رمز به صورت کد شده و با یک الگورتیم مناسب در بانک اطلاعاتی نگهداری می‌شوند) یا تدابیری جهت جلوگیری از تزریق دستور به کارگزار بانک اطلاعاتی یا تدابیری جهت جلوگیری از سرقت اطلاعات در هنگام نقل و انتقال در شبکه است.

هنگام ورود کاربر به صفحه ورود به سایت، یک مسیر و باند حفاظت شده به وسیله الگوریتم رمزنگاری (SSL) میان رایانه کاربر و مدیر ایجاد می‌شود که همه نقل و انتقال‌های اطلاعات از این مسیر حفاظت‌شده میان این دو رایانه، رد و بدل خواهد شد و این تکنیک دسترسی غیر مجاز به اطلاعات ارسالی و دریافتی را برای کسانی که استراق سمع می‌کنند، ناممکن خواهد کرد.

با رشد سریع اینترنت و کاربردهای آن یکی از مسأله‌های اساسی مدیران وب‌سایت‌ها و شبکه‌ها و همه کاربران، بحث امنیت در اینترنت و روش‌های تامین آن است. مدیر امنیتی شبکه برای برطرف کردن نیازهای امنیتی، نیاز به شناخت نقص‌های امنیتی و انتخاب سیاست‌ها و محصول‌های امنیتی متفاوت دارد.

بنابراین لازم است مجموعه پارامترهای امنیتی در کنار هم قرار گیرند تا بتوانند امنیت را در حد مطلوب برای یک شبکه و سیستم‌های فعال در شبکه و وب‌سایت‌ها، حفظ نمایند.

محرمانه ماندن اطلاعات کاربران، عدم تغییر اطلاعات آنان و در دسترس بودن امکانات وب‌سایت برای کاربران مجاز، احراز هویت کاربران و هم‌چنین کنترل دسترسی کاربران به منابع موجود در

وب‌سایت از اصول بنیادی امنیتی هستند که مدیر وب‌سایت باید برای کاربران احراز هویت شده و کاربران میهمان فراهم می‌نماید.

امنیت در اینترنت، فرآیندی است که هرگز نمی‌توان با اطمینان گفت، راهی برای نفوذگران جهت دسترسی غیر مجاز به سیستم‌ها و وب‌سایت‌ها وجود ندارد؛ زیرا همیشه نفوذگران در پی شکافی هستند تا از آن برای نفوذ استفاده نمایند.

بنابراین هر شبکه فعال در اینترنت با هر هدفی که بر عهده دارد، بدون نفوذگر نخواهد بود و سرانجام همه گروه کاربران و شبکه‌های مرتبط با آن نیز تحت تأثیر، قرار خواهند گرفت و با به‌روز نگاه‌داشتن دانش و اطلاعات کاربران و شناخت انواع آسیب‌پذیری‌های موجود برای یک شبکه و کاربران وب‌سایت‌ها، می‌توان سطح امنیتی وب‌سایت‌ها و سیستم‌های موجود در شبکه را در حد مطلوب نگاه داشت.

از جمله آسیب‌پذیری‌هایی که متوجه یک سیستم واحد است، کلمه‌های عبور قابل حدس، استفاده از نرم‌افزارهای قدیمی و مدیریت ضعیف سیستم، بی‌دقتی در حفظ اطلاعات محرمانه و عدم آموزش کاربرانی که از دانش امنیتی کافی برخوردار نیستند و اطمینان به برنامه‌ها و داده‌هایی که از جانب کاربران و شبکه‌های مرتبط وارد شبکه می‌شوند، نام برد. برای پیکربندی درست و تست آسیب‌پذیری ابزارها، سیستم‌ها و برنامه‌های موجود و وب‌سایت‌ها، نیاز به سیاست‌های امنیتی وجود دارد تا یک راه‌حل اصولی، ارایه دهد که می‌بایست این راه‌حل‌ها به وسیله همه کاربرانی که به نوعی با سیستم‌های اطلاعاتی و وب‌سایت‌ها در ارتباط هستند، رعایت و اجرا شود.

مهم‌ترین هدف یک سیاست امنیتی، دادن آگاهی لازم به همه کاربران و مدیران مرتبط با وب‌سایت در رابطه با نحوه استفاده درست از پارامترهای موجود، جهت حفظ سرمایه‌های اطلاعاتی در وب‌سایت است. اطلاعاتی که در حالت عادی میان کاربران در دنیای اینترنت، رد و بدل می‌شوند به گونه‌ای هستند که یک نفوذگر یا خرابکار حرفه‌ای می‌تواند آنها را مشاهده کند و برای اهداف خود مورد سوءاستفاده قرار دهد.

برای مثال: در یک خرید اینترنتی، زمانی که قصد دارید برای پرداخت به حساب بانکی خود وارد شوید، وب‌سایت از شما رمز عبور می‌خواهد؛ حال اگر سایت مورد نظر فاقد برنامه‌های امنیتی لازم باشد، ممکن است، اطلاعات شما در میانه راه بدون آن‌که متوجه شوید، دزدیده شوند.

برای ایجاد امنیت در وب‌سایت، نیاز به شناخت کاربران غیر مجاز که «نفوذگر» نامیده می‌شوند، وجود دارد. نفوذگرها، همیشه در پی شکار ضعف‌های موجود در یک سیستم هستند. اگر یک جامعه اطلاعاتی داشته باشیم، افرادی می‌توانند به این اطلاعات دستیابی بیابند که مجوز لازم را داشته باشند؛ نفوذگران، افرادی هستند که مجوز دستیابی به این اطلاعات را ندارند. بنابراین آن‌چه از این نگرش به دست می‌آید، این است که نفوذگرها به دنبال پیدا کردن حفره‌های جدید برای حمله هستند. منبع اصلی نفوذگرها به جز هوش آنها، کدهای کامپیوتری است.

تنها تعداد اندکی از نفوذگرها شخصا اقدام به برنامه‌نویسی می‌کنند. برخی از نفوذگران به دنبال کدهای آماده در اینترنت می‌گردند تا به سیستم‌های کامپیوتری و شبکه‌ها نفوذ کنند. بنابراین نباید به نفوذگر فرصت نفوذ به سیستم را داد؛ چون گاهی یک حفره کوچک، کافی است تا نفوذگران از آن برای حمله استفاده کنند.

انواع مختلفی از حملات وجود دارد که نفوذگران ممکن است از آنها جهت نفوذ استفاده کنند؛ این حملات در دو دسته کلی به «حملات فعال» و «حملات غیر فعال» دسته‌بندی می‌شوند.

ممکن است نفوذگرها به منابعی از اطلاعات دستیابی نمایند اما اقدام به تغییر محتوای اطلاعات منبع نکنند؛ مانند: شنود ساده یا آنالیز ترافیک که این نوع حملات از حملات غیر فعال هستند؛ این نوع حملات به دلیل مخفی عمل نمودن و مخفی ماندن، خطرناک‌ترین حملات به شمار می‌آیند و پیامدهای این نوع حملات آشکار شدن اطلاعات محرمانه و یا فایل‌های اطلاعاتی برای یک مهاجم بدون اطلاع و آگاهی کاربر است یا این‌که نفوذگرها افزون بر دستیابی به اطلاعات، تغییرهایی نیز اعمال می‌نمایند که انجام این تغییرها مجاز نیست و شناسایی رخداد این حملات فرآیندی، امکان‌پذیر است، این حملات می‌توانند از طریق ستون فقرات یک شبکه برای سوءاستفاده اطلاعاتی، نفوذ در یک قلمرو محرمانه و حفاظت شده و یا حمله به یک کاربر احراز هویت شده (در زمان ارتباط با یک ناحیه حفاظت‌شده) امکان‌پذیر باشد.

از این نوع حملات، می‌توان به تغییر هویت، پاسخ‌های جعلی، تغییر پیام و عدم پذیرش سرویس (DOS) و افشای اطلاعات اشاره نمود. با توجه به بررسی مکانیزم احراز هویت در این مقاله به بررسی رایج‌ترین نوع حمله فعال، یعنی تغییر پیام (Message Modification) که ارتباط مستقیم با احراز هویت دارد، پرداخته می‌شود.

از آن‌جایی که انواع متنوعی از ترافیک بر روی شبکه انتقال می‌یابند و هر یک از این ترافیک‌ها و پروتکل‌ها از شیوه‌هایی برای مدیریت جنبه‌های امنیتی خود استفاده می‌کنند. بنابراین نفوذگر با اطلاع از پروتکل‌های مختلف می‌تواند برای هر یک از این انواع ترافیک، نوع خاصی از تغییر پیام‌ها و در نتیجه حملات را اتخاذ کند.

این حملات تنها دستیابی به اطلاعات را هدف نمی‌گیرند بلکه با اعمال تغییرهای خاص، دو طرف را گمراه می‌سازند و مشکل‌هایی را برای سطح دسترسی مختلف (کاربران میهمان یا کاربران احراز هویت شده و مدیران) ایجاد می‌کنند.

یکی از مکانیزم‌هایی که در وب‌سایت‌ها دسترسی کاربران را مدیریت و کنترل می‌کند و می‌تواند برای جلوگیری از حمله از نوع تغییر پیام مؤثر باشد، مکانیزم احراز هویت است؛ این مکانیزم، نام کاربری و کلمه عبور ارایه شده از سوی کاربر را دریافت کرده و سپس سیستم آن را با بانک اطلاعاتی مختص کدهای شناسایی کاربری مقایسه کرده و پذیرش و عدم پذیرش دسترسی به منابع را صادر می‌کند.

در این مقاله یک مکانیزم احراز هویت لایه‌ای معرفی می‌شود تا در صورتی که یک نفوذگر، کلمه رمز اولی را به دست آورده باشد، باز هم کلمه عبور دوم و سؤال امنیتی لایه سوم، پرسیده می‌شود و اجازه ایجاد تغییرهای اساسی در سطح وب‌سایت را به نفوذگر نمی‌دهد. ساختار این مقاله بدین صورت است که بخش دوم این مقاله، شامل معرفی مکانیزم احراز هویت و انواع آن است و در بخش سوم و چهارم مقاله، احراز هویت لایه‌ای را بیان می‌نماییم و به بررسی راهکارهای لازم در خصوص استفاده از این روش در وب‌سایت‌ها می‌پردازیم.

## ۲- مکانیزم احراز هویت

هم‌چنان که در مقدمه بیان شد، امنیت وب‌سایت‌ها باید از دستیابی افراد غیر مجاز یا نفوذگرها محافظت گردد. بنابراین یکی از نیازمندی‌های امنیتی وب‌سایت‌ها، کنترل دسترسی کاربران به داده‌ها و بخش‌های مختلف سایت است.

روش‌های مختلفی برای محافظت داده‌ها از دستیابی نفوذگران وجود دارد. از جمله مکانیزم‌های کنترلی در وب‌سایت‌ها، پیاده‌سازی سرویس امنیتی AAA است که بر دسترسی کاربران به منابع شبکه و منابع وب‌سایت‌ها، مدیریت مستقیم و متمرکز، خواهد داشت.

AAA یک مکانیزم امنیتی لایه‌ای را ایجاد می‌کند و سرنام سه کلمه، احراز هویت (Authentication)، اعتبارسنجی (Authorization) و مجوز دستیابی (Accounting) است.

نخستین سطح دسترسی، احراز هویت است که راهی را جهت تشخیص هویت کاربران فراهم می‌آورد که به طور معمول این کار با وارد کردن کلمه کاربری و کلمه عبور درست، قبل از برقراری دسترسی خاص صورت می‌گیرد. AAA سرور مشخصات کاربر را با بانک اطلاعاتی مرکزی خود مقایسه کرده و در صورتی که مطابقت داشته باشد، دسترسی داده می‌شود و در غیر این صورت دسترسی به منابع ناممکن خواهد بود.

در شبکه‌های خصوصی یا عمومی نظیر اینترنت احراز هویت با استفاده از ورود کلمه عبور صورت می‌گیرد. دانستن کلمه عبور در واقع دسترسی کاربر را به منابع مورد نیازش تضمین می‌کند.

از نقص‌های سیستم‌های کامپیوتری می‌توان به دزدیده شدن کلمه عبور، لو رفتن و فراموش کردن آن، اشاره کرد به همین دلیل معامله‌های بانکی و دیگر فعالیت‌های مهم روی اینترنت و شبکه نیاز به سطوح امنیتی دیگر (به غیر از احراز هویت) خواهند داشت.

دومین سطح دسترسی اعتبارسنجی است که جهت انجام وظیفه‌های خاص پس از ورود به سیستم صورت می‌گیرد. به عنوان مثال: کاربر تصمیم به اجرای دستورهایی روی وب‌سایت می‌گیرد.

بنابراین، پردازش اعتبارسنجی مشخص می‌کندکه آیا کاربر اجازه انجام دادن کاری و یا در اختیار داشتن چیزی را دارد یا خیر؟

در وب‌سایت‌ها، مدیر وب‌سایت، مشخص می‌کند که چه کاربرانی اجازه دسترسی به سیستم را دارند و حدود دسترسی آنها که میزان استفاده کاربر را در طول دسترسی مشخص می‌کند، چقدر است؟

سطح سوم امنیت که مجوز دستیابی است، مشخص می‌کند که کاربر مجوز استفاده از کدام بخش و به چه مقدار اطلاعات در طول برقراری یک جلسه را دارد؛ AAA سرور، درخواست ایستگاه کاری را مبنی بر استفاده از منابع شبکه، دریافت می‌کند و سپس شروع به احراز هویت کاربر می‌نماید، سپس حدود دسترسی کاربر را به ایستگاه کاری ارسال می‌نماید.

از مکانیزم‌های کنترلی یادشده در این مقاله به بررسی مکانیزم احراز هویت پرداخته می‌شود. ابتدا مکانیزم احراز هویت را بررسی کرده و انواع روش‌های پیاده‌سازی و برقراری احراز هویت را بیان می‌کنیم، سپس چالش‌ها و معایب احراز هویت را بررسی کرده و در بخش های سوم و چهارم راهکار جدیدی برای بهبود مشکل معرفی می‌کنیم.

مکانیزم احراز هویت یکی از اساسی‌ترین توابعی است که دسترسی کاربران در شبکه و وب‌سایت‌ها را مدیریت می‌کند. برای محدود نمودن کاربرانی که مجوز دسترسی به منابع را دارا هستند و هم‌چنین عدم دسترسی کاربران غیر مجاز به منابع در وب‌سایت، می‌توان از این فرآیند امنیتی استفاده نمود.

این مکانیزم کاربر را شناسایی کرده و پس از تأیید هویت آنان، امکان دستیابی به برنامه با توجه به مجوزهای تعریف شده را فراهم می‌کند. بنابراین زمانی که کاربر یا فردی از خارج سیستم، می‌خواهد به اطلاعات و مدارک موجود در درون سیستم کامپیوتری دستیابی داشته باشد. نخستین مرحله در فرآیند کنترل، دستیابی کاربران به منابع احراز هویت است.

احراز هویت ممکن است، شامل موارد زیر باشد: اطلاعاتی که یک فرد آن را می‌داند (کلمه رمز، نام کاربری) یا چیزی که یک فرد در اختیار دارد (USB کارت‌های خاص) و یا مشخصه‌های موجود در یک فرد (اثر انگشت، DNA، خصوصیات چشم، خصوصیات صورت و...) است.

مکانیزم احراز هویت در دو دسته «بیومتریک» و «غیر بیومتریک» مطرح می‌شود. تکنولوژی بیومتریک، روش‌های شناسایی یک فرد بر مبنای خصوصیات فیزیکی و رفتاری وی است.

این تکنولوژی از دو مرحله استفاده می‌کند، مرحله اول یادگیری (Enrolment) است که در آن با استفاده از سیستم‌های خاص، نمونه‌های مربوط به یک شخص گردآوری شده و در یک بانک اطلاعاتی ذخیره می‌شود.

در مرحله بعد، این اطلاعات در مورد شخص مورد نظر اجرا شده و با مشخصات ذخیره شده، مقایسه می‌شود و سپس درستی و نادرستی آن مشخص می‌شود که اثر انگشت، خصوصیات صورت، عنبیه چشم، امضای حرکتی، DNA و... از جمله این موارد هستند.

امروزه در امور مربوط به امنیت مکان‌هایی مانند دانشگاه‌ها، فرودگاه‌ها، وزارتخانه‌ها و حتی شبکه‌های کامپیوتری، استفاده از روش‌های بیومتریک در تشخیص هویت و یا تأیید هویت افراد بسیار متداول شده است.

سیستم‌های پیشرفته حضور و غیاب اداره‌ها، سیستم‌های حافظتی ورود و خروج مکان‌های خاص، نوت‌بوک‌های مجهز به Finger Print و... از روش‌های مختلف تشخیص هویت بیومتریک استفاده می‌کنند.

به عنوان مثال: پاسپورت‌های بیومتریک، دگرگونی اساسی در نظام تهیه پاسپورت و کنترل ورود و خروج مسافران در سراسر دنیا ایجاد خواهند کرد. جعل پاسپورت بیومتریک، بسیار دشوارتر از انواع کنونی آن خواهد بود.

سیستم‌های بیومتریک، هویت هر فرد را در الگوهای ویژه‌ای خلاصه می‌کند و اثر انگشتان، ویژگی چشم، صورت، صدا و دیگر خصوصیات فیزیکی را در قالب الگوریتم‌های ریاضی بر روی یک تراشه و یا یک نوار ویژه ثبت و ضبط می‌کند.

بدین ترتیب، هنگامی‌که مسافران به مرکزهای ورودی کشور می‌رسند، انگشتان خود را در مقابل یک اسکنر ویژه قرار داده، هم‌زمان چهره آنان نیز توسط اسکنر بیومتریک دیگری مورد بررسی دقیق قرار می‌گیرد و مشخصات به دست آمده با الگوها و ویژگی‌های ثبت شده در پاسپورت مقایسه می‌شود.

روش‌های بیومتریک، روشی مطمئن برای شناسایی کاربر مورد نظر است و به راحتی قابل جعل نبوده و استفاده از آن برای کاربران راحت‌تر است اما نصب و پیاده‌سازی سیستم‌های بیومتریک در برخی اداره‌ها و سازمان‌ها برای شناسایی کاربر مورد نظر، دارای تکنولوژی پیچیده و راه حل امنیتی پر هزینه‌ای است و هم‌چنین استاندارد خاصی برای آن در صنعت وجود ندارد و سیستم‌های آن، قابل استفاده از راه دور نیستند و امکان تشخیص نادرست نیز در احراز هویت بیومتریک وجود دارد.

یک تشخیص اشتباهی، زمانی روی می‌دهد که به کاربری که نباید مجوز دسترسی داده شود با دسترسی وی به داده‌ها موافقت می‌شود. در حالی که در رد کردن اشتباهی به کاربری که باید مجوز دسترسی داده شود با دسترسی وی به داده‌ها موافقت نمی‌شود.

هم‌چنین زمانی که انسان دچار تغییرهای جسمانی می‌شود. به طور مثال: اگر شخص بیمار شود به علت تب و گلو درد، صدای او تغییر می‌کند و یا اگر سر و صدای زیادی در محیط باشد با روش بیومتریک، دیگر با تشخیص صدا، نمی‌توان به درستی احراز هویت شود یا افرادی که در صنایع شیمیایی کار می‌کنند، اثر انگشت بیشتر آنها تحت تأثیر قرار می‌گیرد؛ بنابراین در این شرکتها نباید دیگر از مدل احراز هویت اثر انگشت استفاده کنند.

هم‌چنین چون اطلاعات روش بیومتریک، شامل مشخصات افراد است و این مشخصات غیر قابل تغییر است، دزدیدن آن اطلاعات مشکل‌هایی را به وجود خواهد آورد.

در کل، سیستم‌های احراز هویت بیومتریک همیشه معتبر نیستند و در هر زمانی قابل اعمال نخواهند بود در حالی که مشکل‌های ذکر شده در روش غیر بیومتریک وجود ندارد؛ چون با انتخاب کلمه عبور مناسب، می‌توان دسترسی به منابع را محدود کرد.

کلمه‌های عبور با استفاده از توابع رمز یک طرفه و از طریق مکانیزم پاسخ - مجادله‌ای، کاربران را احراز هویت می‌کند؛ بدین صورت که کلمه رمزی را که کاربر در ابتدا تعیین می‌کند، توسط یک رشته تصادفی رمزنگاری شده و در سیستم ذخیره می‌شود و وقتی کاربر برای ورود، کلمه رمز را وارد می‌کند. همین مسیر در هنگام احراز هویت طی شده و حاصل آن با مقدار ذخیره شده، مقایسه می‌شود و سرانجام درخواست کاربر برای ورود پذیرفته و یا رد می‌شود.

از دیگر ویژگی‌های غیر بیومتریک، احراز هویت است که نشانه‌ای سخت‌افزاری بوده که برای دسترسی به سرویس‌های شبکه‌ای از آن استفاده می‌شود و به صورت یک کارت هوشمند بوده و با استفاده از نشانه امنیتی می‌توان احراز هویت قوی‌تری ایجاد نمود که افزون بر کلمه عبور، اطلاعات دیگری مربوط به نشانه را برای احراز هویت در اختیار سیستم قرار می‌دهد.

به عنوان مثال: یک شرکت امنیتی، محصولی با نام SecureID را ارایه کرده است که دارای نمایشگری است و در هر دقیقه عددی متفاوت را نمایش می‌دهد و مالک این نشانه برای استفاده از سیستم، ابتدا کلمه عبور خود را وارد کرده و سپس عددی که توسط SecureID نمایش داده شده است را در اختیار سیستم قرار می‌دهد و سیستم این اطلاعات را از طریق سرویس‌دهنده احراز هویت، بررسی کرده و با انجام محاسبات مخفی، مشخص می‌کند که آیا فرد مجاز به دسترسی به سیستم است یا خیر؟

ایراد این روش نیز این است که در کاربردهای شبکه‌ای و سرورها مفید بوده و قابل استفاده در وب‌سرورها و سایت‌های اینترنتی نیست. مدیران وب‌سایت‌ها برای دستیابی به وب‌سرور از نام کاربری و کلمه رمز استفاده می‌کنند که با توجه به نام کاربری، سطح دسترسی به بخش‌های مختلف تقسیم می‌شود اما این تکنولوژی نیز به علت یک لایه‌ای بودن دارای معایبی است.

برای مثال: در صورتی که رمز، دزدیده یا فراموش شده یا توسط نفوذگران هک شود، این روش‌ها قابل اطمینان برای احراز هویت کاربران نخواهد بود؛ زیرا نفوذگر به راحتی وارد وب‌سایت شده و به داده‌ها دسترسی پیدا خواهد کرد.

برای حل این مشکل، لایه دوم را برای احراز هویت کاربران قرار می‌دهیم که در بخش های سوم و چهارم مقاله مطرح خواهیم کرد.

## ۳- محدود کردن کاربران

در دسترسی آزادانه به بخش مدیریت، نفوذگران با وارد کردن کدهای مخرب به جای نام کاربری و کلمه عبور می‌توانستند، وارد سایت شوند برای جلوگیری از این نفوذ از اجزای AJAX ورودی‌ها را فیلتر می‌کنیم که حساس به کدهای مخرب شود و منوی مدیریت سایت را از دید کاربران مخفی می‌کنیم و در این پیشنهاد، ابتدا در پایگاه داده به صورت درخواستی، اطلاعات را برای مدیر تعریف می‌کنیم، سپس به صورت شکل ذیل کلمه عبور مدیر یا کاربر خواسته می‌شود.


**شکل (۱) طریقه ورود اطلاعات اولیه**

پس از احراز هویت، کدی را که نوشتیم اگر کاربر، مدیر باشد، منوی ورود به مدیریت سایت به صورت رنگ قرمز نمایش داده می شود.


**شکل (۲) فعال شدن منوی مدیریت**

سپس کلیک بر روی آن به سایت دیگری که شبیه نام این سایت است لینک داده می‌شود و در آنجا جدول‌هایی را برای کلمه عبور کاربری و سؤال امنیتی درست می‌کنیم و بعد از واگذاری سایت به مسؤول مربوطه، اطلاعات و رمز خود را تغییر می‌دهند. بدین منظور از دو جدول در پایگاه داده استفاده می‌کنیم تا جدول‌های یاد شده از رابطه(Relation ship) استفاده نمایند و اگر کسی قصد نفوذ را داشته باشد در هنگامی که به یکی از جدول‌ها دسترسی پیدا کند، فکر می‌کند این رمزها همان کلمه عبور هستند؛ بدین روی اگر نفوذگر، قصد تخریب را داشته باشد، نمی‌تواند اطلاعات را حذف کند؛ چون جدول‌ها با یکدیگر به صورت رابطه‌ای ارتباط دارند؛ بدین منظور نفوذگران امکان تغییرهایی در پایگاه داده، نمی توانند داشته باشند.

## ۴- احراز هویت لایه‌ای

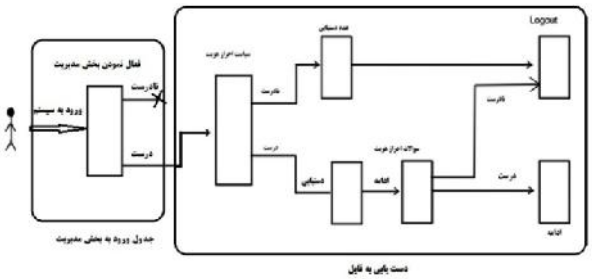
مطابق با مطالب یاد شده در بخش دوم، احراز هویت بیومتریک نمی‌تواند به عنوان راهکار امنیتی برای کنترل دستیابی به داده‌ها مطرح شوند؛ افزون بر آن، مکانیزم احراز هویت مبتنی بر نشانه (token) که از کلمه‌های رمز و نام کاربری استفاده می‌کنند با احتمال لو رفتن کلمه رمز، چندان قابل اطمینان نیستند. در بستر اینترنت مجموعه‌ای از سرورهای عمومی هم‌چون وب‌سرورها وجود دارد که به طور کلی بخش عمومی شبکه اینترنت را تشکیل می‌دهند و به عموم کاربران اینترنت سرویس می‌دهند.

این مجموعه در محیط محصور شده‌ای قرار می‌گیرد و این محیط، بخش عمومی را از بخش خصوصی یا محرمانه که برای سرویس‌دهی به کاربران ثبت نام کرده و در وب‌سایت، پیاده‌سازی شده، تفکیک می‌نماید.

بخش عمومی سایت توسط فیلتر عمومی محافظت می‌شود تا از کارایی سرویس‌دهنده، کاسته نشود و بخش خصوصی وب‌سایت توسط لایه‌ای محافظت می‌شود که ضمن غیر قابل نفوذ نمودن آن از خارج، بتوان ارتباط کاربران ثبت نام کرده را به وب‌سایت فراهم نمود.

در ساختار پیشنهاد شده در این مقاله یک نفوذگر برای برقراری ارتباط با سیستم داخلی وب‌سایت سه مانع عمده در سر راه دارد، سه لایه از مکانیزم احراز هویت وجود دارد به طوری که اگر نفوذگر به نحوی از لایه اول این مکانیزم با به دست آوردن شماره شناسایی کاربر و یا رمز عبور با به کارگیری یکی از روش‌های نفوذ، عبور نماید، باید برای ادامه فعالیت از جدول دیگری که باز هم رمز عبور و نام کاربری دارد، بگذرد و در لایه آخر که برای دسترسی به حذف و اضافه مدیریت فایل طراحی شده است، باید به سؤال امنیتی که کاربر در موقع ثبت نام پر کرده، پاسخ دهد.

به عنوان مثال: نفوذگر باید رمز دوم را وارد نماید، اگر پاسخ او درست باشد، سیستم اجازه ورود به قسمت مورد نظر برای دسترسی به منابع مورد نیاز را می‌دهد؛ در غیر این صورت به عنوان کاربر ناشناس شناخته می‌شود و به صفحه اول برگشت داده می‌شود که این عملیات در لایه سوم مکانیزم احراز هویت لایه‌ای انجام می‌گیرد. شکل (۳) ساختار کلی مورد استفاده در این مقاله را توضیح می‌دهد.




**شکل (۳) مکانیزم احراز هویت لایه‌ای**

سطح احراز هویت این مکانیزم به سطح ریسک تراکنش درخواستی از سوی کاربر وابسته است و تغییرها مطابق با آن صورت می‌گیرد.

در ضمن هر کاربر یک صفحه پروفایل شخصی در سایت دارد و این صفحه بیانگر اطلاعات عمومی همان شخص است که کاربر آن را هنگام ثبت نام پر کرده است.

بخش پروفایل، یک امکان اختیاری است و کاربران می‌توانند تنها مواردی که مایل به نمایش عمومی آن هستند را در فرم پروفایل خود وارد کرده و هر زمان نیز نمایش عمومی پروفایل را غیر فعال کنند.

شکل (۴) نمونه‌ای از یک فرم ثبت نام را نشان می‌دهد که اطلاعات وارد شده در این فرم را در پروفایل کاربر ذخیره می‌کند.

**شکل (۴) مراحل ثبت نام و تهیه پروفایل**

هنگام ثبت نام کاربر، یک سؤال امنیتی از او پرسیده می‌شود و به همراه پروفایل او در جدول‌های جداگانه‌ای ذخیره می‌شود اما این سؤال امنیتی در بخش پروفایل قابل مشاهده نیست. هنگامی که یک نفوذگر از طریق فرم‌هایی مانند فرم شکل (۱) وارد سیستم شود به نحوی نام کاربری و کلمه رمز را با استفاده از روش‌های مختلف به دست آورده

است که منوی شکل (۲) برای آن فعال می‌شود و پس از کلیک بر روی آن لینک داده می‌شود به فرم شکل (۵) که به نحوی نام کاربری و کلمه رمز را با استفاده از روش‌های مختلف به دست آورده است و مکانیزم احراز هویت لایه دوم نیز آن را تأیید می‌کند.


**شکل(۵) احراز هویت لایه دوم**

پس از مدتی همان سؤال امنیتی که در هنگام پر کردن فرم ثبت‌نام جواب داده است از او پرسیده می‌شود که این مرحله، همان احراز هویت لایه سوم است. (شکل ۶)


**شکل(۶) احراز هویت لایه سوم**

اگر سؤال امنیتی درست جواب داده شود، کاربر، همان کاربر اصلی تشخیص داده شده و اجازه ادامه کار و دسترسی به منابع را خواهد داشت، در غیر این صورت این کاربر، یک کاربر ناشناس است که هدف او نفوذ به وب‌سایت است؛ بنابراین اجازه دستیابی به بخش‌های مختلف وب‌سایت به وی داده نمی‌شود. برای مثال: با استفاده از این روش پیاده‌سازی حساب‌های بانکی که از طریق وب‌سایت، عملیات بانکی را انجام می‌دهند در نظر بگیرید، در این سایت، فرد هنگام ثبت نام، همه مشخصات خود را در یک پروفایل پر کرده و به همراه آن به یک یا دو سؤال امنیتی سیستم(رمز دوم) از جمله سؤال مربوط به دوران دبستان و یا علاقه فرد به ورزش خاص، پاسخ می‌دهد و همه این داده‌ها در بانکهای اطلاعاتی ثبت می‌شود اما برای عبور از لایه های مکانیزم احراز هویت لایه‌ای، لازم است به سؤال های امنیتی که در مرحله های مختلف پرسیده می‌شود، پاسخ دهد و پاسخ وی با پاسخی که فرد در هنگام ثبت نام در پروفایل ارایه داده، مقایسه می‌شود اگر پاسخ او درست باشد، اجازه دسترسی به داده‌ها و انتقال حساب بانکی و هر عملیات دیگر داده می‌شود. اما اگر با مقایسه‌ای که بانک اطلاعاتی انجام داده، نتیجه اشتباه باشد و همچنین برنامه‌ای هم می‌نویسیم که اگر در حدود ۱۰ دقیقه از سایت استفاده نکند کاربر به صفحه اول برگشت داده می‌شود. ما در این‌جا از دو سرور با تکنولوژی‌های مختلف بهره گرفتیم و بخش مدیریت را با PHP که روی هاست Linux و پوسته آن را با ASP.net که روی هاست ویندوز سرور هست، طراحی کردیم و با این کار تلاش نمودیم، نفوذگران را گمراه کنیم و شرطهایی را در سایت نوشتیم که کابر نتواند تشخیص دهد، روی کدام سرور هست؛ هم‌چنین با این کار در شناساندن سایت به گوگل در صفحه اول کمک نمودیم (SEO) و نوار آدرس سایت را با فرمت HTML نمایش دادیم تا کاربران و نفوذگران از طراحی سایت به زبانهای مختلف با خبر نشوند و باعث امنیت بیشتر هم بشود.

از طرف دیگر امنیت در وب‌سایت‌ها یکی از اساسی‌ترین مباحث در بستر اینترنت است؛ در این بستر گاهی وقت‌ها نمی‌توان راهکار ارایه کرد که در آن صورت، امنیت با ارزش منطقی یک در آن وجود دارد اما راهکار ارایه شده در این مقاله می‌تواند تا حدودی ایرادهای قبلی موجود در وب‌سایت‌ها را پوشش دهد و باعث افزایش امنیت در حوزه دستیابی به اطلاعات شود؛ چون ما از امنیت‌های ترکیبی استفاده می‌کنیم، مثلا استفاده از کیبرد روی فرم‌ها و کنترل آپلود حجم زیادی از فایل و ارسال فایل‌های مخرب و کنترل خطاها که باعث مخفی نگاه داشتن نسخه‌ها و زبان‌های مورد استفاده می‌شود و نیز دستورها استفاده شده را در سایت کنترل می کنیم.

## ۵- نتیجه‌گیری

روش‌های مختلفی برای ایجاد امنیت در سطح وب‌سایت‌ها وجود دارد تا از طریق آنها بتوان داده‌های موجود را از دستیابی نفوذگران محافظت کرد. ایراد روش بیومتریک این است که نمی‌توان در همه کاربردها مثلا وب‌سایت از آن استفاده کرد. با بهره‌گیری از روش غیر بیومتریک که فقط از نام کاربری و کلمه رمز استفاده می‌کند، نیز در این مقاله به بررسی ایجاد امنیت از طریق احراز هویت لایه‌ای پرداختیم و نشان دادیم زمانی که یک کاربر از طریق نام کاربری و کلمه رمز، وارد سیستم می‌شود، باید باز هم از او، کلمه عبور و در آخر سؤال امنیتی پرسیده شود تا سطح امنیت بالاتری ایجاد شود.

در نتیجه نفوذگری که با دزدیدن نام کاربری و کلمه رمز، وارد بخش مدیریت وب‌سایت شده است، نمی‌تواند به فعالیت خود در سطح وب‌سایت ادامه دهد. بنابراین راهکار ارایه شده، توانسته است ایراد قبلی دسترسی به وب‌سایت‌ها را پوشش دهد و باعث افزایش امنیت در حوزه دستیابی به اطلاعات شود. برای امنیت بیشتر نیز از ۲ سرور استفاده کردیم که اگر اولی خراب و یا هک شد، لینک به دومی داده شود اما اگر دومی خراب شد با کنترل خطا، پیغامی مبنی بر اینکه سایت در حال به‌روزرسانی است، ارایه شود تا ما در فرصت مناسب اطلاعات هک شد پشتیانی که از اطلاعات آنها گرفتیم را برگردانیم.

## مراجع


[۱] جودی، شاپور، ارایه روشی برای ایجاد امنیت بالاتر در وب‌سایت‌ها با استفاده از مکانیسم‌های احراز هویت لایه‌ای، دانشگاه فردوسی مشهد، ۱۳۹۰.

[۲] آراسته، محمد، مکانیسم‌های احراز هویت و نحوه پیاده‌سازی آن در سطح برنامه کاربردی، مرکز آپای دانشگاه یزد، ۱۳۸۷.

[۳] آراسته، محمد، اصولی جهت امن کردن مکانیزم احراز هویت علیه حملات کاربردی، مرکز آپای دانشگاه یزد، ۱۳۸۷.

[4] QT Worldtel Inc, "Centralized Out - Of - Band Authentication System", Southeast Europe Cybersecurity Conference Sophia, Bulgaria September 8-9, 2003.

[5] N.S,J.H, "Authentication Technologies for the Blind or Visually Impaired", 2008.

[6] ISO/IEC JTC 1/SC 36 Biometrics, American National Standards Institute, 2006.

[7] V.M,Z.R, "BIOMETRIC AUTHENTICATIONSECURITY AND USABILITY", 2002.