ISSN: 2745-3673
http://www.Rcsj.ir

مجله علمی پژوهش در علوم رایانه(سال پنجم)
شماره ۲۰ / زمستان ۱۳۹۹ / ص ۵۲- ۴۴

ارائه یک الگوی امنیتی جهت حفظ حریم خصوصی در وب با استفاده از الگوریتم کربروس

مریم زنده بودی[۱]، مهدی تیموری[۲]

[۱] دانشجوی کارشناسی ارشد الکترونیک دیجیتال، دانشگاه آزاد اسلامی واحد تهران غرب، تهران، ایران

[۲] استاد یار دانشکده فنی و مهندسی گروه برق، دانشگاه آزاد اسلامی واحد تهران غرب، تهران، ایران.

نام نویسنده مسئول:
مریم زندی بودی

تاریخ دریافت: ۱۳۹۹/۸/۴
تاریخ پذیرش: ۱۳۹۹/۱۰/۹

چکیده

امروزه با توجه به رشد روز افزون شبکه‌های اینترنتی و محیط‌های تحت وب، تعداد استفاده کنندگان از این محیط‌ها به طور گسترده در حال افزایش است. این افزایش کاربران دارای دو جنبه مثبت و منفی است. مثبت از این جهت که عموم مردم به راحتی می‌توانند بواسطه این محیط فعالیت‌های روزمره خود را انجام دهند و منفی از این جهت که بدلیل وجود افراد مخرب در این محیط‌ها، احتمال سرقت اطلاعات کاربران از سوی این افراد افزایش می‌یابد. از این رو حفظ حریم خصوصی افراد و تامین امنیت کاربران این محیط‌ها به عنوان اصلی ترین دغدغه ارائه دهندگان محیط‌های تحت وب می‌باشد. در این راستا متخصصان امنیت اطلاعات بر این باور هستند که بهترین دفاع در قبال نفوذگران، ایجاد لایه‌های امنیتی و سیستم‌های تشخیص نفوذ قدرتمند در شبکه است. یکی از راه کارهای ایجاد لایه امنیتی در شبکه‌ها و محیط‌های تحت وب، استفاده از تکنیک‌ها و الگوریتم‌های رمزنگاری است. در این پژوهش قصد داریم تا بواسطه الگوریتم کربروس یک الگوی امنیتی را جهت حفظ حریم خصوصی کاربران در محیط-های وب ارائه دهیم. الگوریتم کربروس فرآیند امن سازی را از طریق دریافت آدرس‌ها، رمز عبورهای مطمئن و ارائه بلیط انجام می‌دهد.

واژگان کلیدی: وب- امنیت- حریم خصوصی- الگوریتم کربروس- رمزنگاری

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

در دنیای کنونی، اینترنت و محیط‌های تحت وب به عنوان یک رسانه ایده آل جهت انتشار فرآیند الکترونیکی محسوب می‌شوند. بنابراین محیط این رسانه می‌بایست دارای ویژگی‌هایی همچون قابلیت تعامل، سرعت عمل و نامحدود بودن باشد. این محیط که به عنوان یک وسیله ارتباطی جدید و پویا شناخته می‌شود، به سرعت از محیط دانشگاهی وارد عرصه عمومی شده است. لازم به ذکر است که محیط وب به عنوان یکی از شبکه‌های رایانه‌ای، فرصت‌های جدید و چشمگیری را جهت تضمین آزادی بیان ایجاد کرده است و نوعی ارتباط راحت را فراهم کرده است[8,5].

دلیل اصلی موفقیت و افسون جاذبه عظیم اینترنت و محیط‌های تحت وب، تبادل اطلاعات در سراسر جهان است. اما این آزادی اغلب برای کسانی که اطلاعات با ارزشی را در دنیای مجازی و وب منتقل می‌کنند مشکل ایجاد می‌کند. بنابراین یکی از مهمترین نگرانی‌ها و درواقع دغدغه اصلی کاربران وب، حفظ حریم خصوصی آنها در این محیط می‌باشد (حفظ حریم افراد در قبال نفوذ افراد مخرب به شبکه). از این رو ارائه دهندگان خدمات وبتلاش‌های زیادی در جهت افزایش ضریب ایمنی این محیط‌ها انجام داده و الگوها امنیتی، مدل‌های رمزنگاری و سیستم‌های تشخیص نفوذ (دیواره آتش) متعددی را برای حفظ این حریم ارائه نموده‌اند. ما نیز قصد داریم تا بواسطه انجام این پژوهش و با بهره گیری از الگوریتم کربروس[1]، مدلی را جهت حفظ حریم خصوصی افراد در محیط‌های تحت وب ارائه دهیم.

سیاست گذاری و حمایت از حریم خصوصی

شبکه‌های اینترنتی تاکنون چالش‌های اجتماعی شدیدی را در حوزه مالکیت معنوی و حریم خصوصی افراد ایجاد کرده‌اند. با آنکه فناوری و خدمات رایانه‌ای بطور دائم در حال رشد و تکامل هستند، اما بسیاری از این چالش‌ها همچنان باقی مانده و مرتفع نشده‌اند. به همین دلیل دولت‌ها باید اهداف، اصول و ارزش‌هایی را جهت فعال سازی نظام‌های ارتباطی معرفی نمایند. از این رو همه دولت‌ها در سراسر جهان درصدد حل مسألهدشوار طرح قانون جهت حفظ حریم خصوصی هستند. بطور کلی تلاش-های دولت‌ها برای تعیین مقررات نحوه استفاده از اطلاعات مربوط به حریم خصوصی افراد در محیط‌های تحت وب رامی‌توان بر اساس میزان حفاظت از این حریم ارزیابی کرد [5,6].

امنیت

در دنیای امروز، مفهوم امنیت به عنوان یک مسألهکاملاً حیاتی برای محیط‌های تحت وب قلمداد می‌شود. از این رو به تدریج و با پیشرفت جوامع بشری، محدوده امنیت نیز ابعاد گسترده‌تری یافته و مفاهیمی همچون حریم خصوصی، امنیت مالی، امنیت سیاسی و غیره را شامل شده است. این تحول بزرگ باعث بروز محدودیت‌های فراوانی می‌شود. به نحوی که امنیت مجازی یا امنیت حریم خصوصی در فضای سایبر به عنوان مهمترین این محدودیت‌ها شناخته می‌شوند. بطور کلی ساختار امنیتی در فضای وب و سایبر می‌بایست بر مبنای چهار فاکتور اصلی باشد. این فاکتورها به شرح زیر هستند [9].

محرمانگی

بر اساس این فاکتور، تنها فرستنده و گیرنده می‌بایست محتوای پیام را درک کنند. در این راستا ابتدا فرستنده پیام را بصورت رمز درآورده و ارسال می‌کند و در انتها گیرنده پس از دریافت این اطلاعات آنها را رمزنگاری می‌کند (استفاده از الگوریتم‌های رمزنگاری).

تایید هویت

با توجه به تعریف، در این حالت فرستنده و گیرنده باید از هویت سمت مقابل (هویت همدیگر) مطمئن شوند (استفاده از تکنیک Nonce)

[1] Kerbros Algorithm

ISSN: 2745-3673
http://www.Rcsj.ir

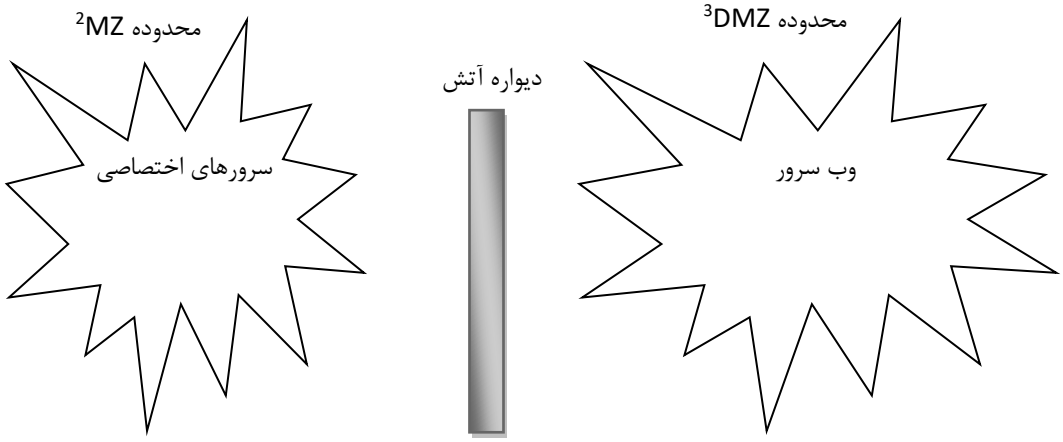
جامعیت پیام

به ازای این فاکتور، فرستنده و گیرنده می‌خواهند از بابت این قضیه اطمینان حاصل نمایند که آیا پیامی که دریافت کرده-اند دارای داده واقعی است ویا اینکه داده‌ها دستکاری شده‌اند. حال اگر داده‌ها دستکاریشده‌اند این قابلیت وجود داشته باشد تا بتوان آنها را شناسایی کرد (استفاده از تکنیک امضای دیجیتال و یا تابع درهم ساز).

در دسترس بودن سرویس مورد نظر

طبق تعریف، در این حالت در هر زمانی که به سرویس موردنظر اعلام نیاز شود، سرویس مذکور باید در دسترس باشد [4].

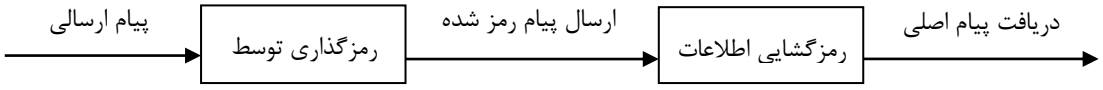
در بحث ایجاد امنیت در شبکه‌های کامپوتری و محیط مجازی، علاوه بر بکارگیری سیستم‌های رمزنگاری می‌توان از سیستم‌های تشخیص نفوذ (دیواره آتش[۲]) نیز استفاده کرد. این سیستم‌ها بر روی شبکه و با بکارگیری ابزارهای متفاوتی، ترافیک زیاد شبکه را ثبت می‌کنند و بدین ترتیب در وقتی مناسب بسته‌های مشکوک را مورد بررسی قرار می‌دهند [10]. شکل (۱) بیانگر ساختار و محدوده عملکرد این سیستم‌های تشخیص نفوذ می‌باشد.



شکل ۱- ساختار سیستم‌های تشخیص نفوذ

رمزنگاری

نکته مهم در ارتباط با مسأله رمزنگاری اینست که به ازای اعمال رمزنگاری بر روی حالت‌هایچهارگانه، این حالت‌ها می-توانند بصورت بهینه تری عمل کنند [۲]. بطور کلی ساختار مربوط به به سیستم رمزنگاری و رمزگشایی بواسطه شکل (۲) قابل ملاحظه می‌باشد.



شکل ۲- ساختار سیستم رمزگذاری و رمزگشایی

لازم به ذکر است که عملیات رمزنگاری پیام دریافتی نیز از طریق رابطه (۱) صورت می‌پذیرد.

[2] Firewall
[2] Militarized Zone
[3] Demilitarized Zone
[4] File Transfer Protocol
[5] Domain Name System

ISSN: 2745-3673
http://www.Rcsj.ir

$$M = K_B(K_M) \quad (۱)$$

که در اینجا :

M= پیام

K_B= کلید مربوط به عملیات رمزنگاری

K_M= کلید مربوط به پیام رمز شده

با توجه به مباحث مطرح شده در این بخش، سعی داریم تا بواسطه این پژوهش یک الگوی امنیتی را ارائه دهیم. از این رو در ادامه و در بخش دوم به ذکر مختصر تاریخچه‌ای از فرآیند حفظ حریم خصوصی و استفاده از الگوهای امنیتی در فضای مجازی و محیط‌های تحت وب می‌پردازیم. سپس در بخش سوم الگوی امنیتی پیشنهادی را شرح می‌دهیم. در بخش چهارم به ارزیابی مدل پیشنهادی با مدل های مشابه پرداخته و در انتها نیز نتیجه اجرای این پژوهش را بیان می‌کنیم

تاریخچه

حفظ حریم خصوصی در فضای سایبر و محیط‌های تحت وب از اهمیت فوق‌العاده ویژه‌ای برخوردار است تا جایی که اکثر دولت‌ها به منظور ایجاد الگوها و سیستم‌های حفاظتی دست به کار شده‌اند و سیاست‌های خاص خود را در پیش گرفته‌اند. از این رو متخصص‌های عرصه شبکه و فناوری اطلاعات نیز بر آن شده‌اند تا الگوهای امنیتی مختلفی را تولید نمایند. در ادامه به ذکر مواردی از این الگوهای امنیتی می‌پردازیم.

در مرجع [۳]، یک معماری مرجع امنیتی جهت حفظ حریم خصوصی افراد در محیط‌های تحت وب و سیستم‌های رایانش ابری[۳] ارائه شده است. این معماری پس از شناسایی نیازمندی‌های سازمان، فعالیت امنیتی خود را عملی می‌کند. همچنین یک معماری امن سمپاد نیز در [۱] و به منظور حفظ حریم خصوصی، محرمانگی و صحت داده ارائه شده است. هدف اصلی این معماری کاهش میزان پیچیدگی فرآیند امنیتی موجود در پایگاه داده‌های برون سپاری شده است.

رمزنگاری بیومتریک[۴] نیز از جمله تکنیک‌های است که به منظور افزایش محرمانگی و حفظ حریم خصوصی در [8] ارائه شده است. همچنین در [7] نیز یک الگوی رمزنگاری مبتنی بر منابع خارجی معرفی شده است. این الگو با مدیریت سازمان کلید خصوصی، فرآیند مذکور را مدیریت می‌کند.

مدل پیشنهادی

همانطور که در ابتدای این نوشتار بیان داشتیم، هدف از انجام این پژوهش ارائه یک الگوی امنیتی بهینه جهت حفظ حریم خصوصی در محیط‌های تحت وب، آن هم از طریق الگوریتم کربروس است. در ادامه ابتدا توضیح مختصری درباره الگوریتم کربروس ارائه داده می‌شود، سپس روش کار این الگوریتم را شرح می‌دهیم.

الگوریتم کربروس

الگوریتم کربروس یک الگوریتم امنیتی است که به منظور انجام عملیات احراز هویت کاربران مجاز موجود در شبکه مورد استفاده قرار می‌گیرد. این الگوریتم پس از تأیید هویت کاربر، امکان ورود آن را به شبکه فراهم می‌کند. کاربران در این سیستم رمزنگاری بلیط‌های ورود را مراکز توزیع کربروس KDC[5] دریافت کرده و پس از برقراری ارتباط با شبکه، این بلیط‌ها را به سمت شبکه ارسال می‌کنند. حال اگر این بلیط‌ها مورد تأیید سیستم کربروس باشند در این صورت کاربران مجوز ورود به شبکه را بدست می‌آورند. درواقع این بلیط‌های ارائه شده توسط الگوریتم کربروس، اعتبار کاربران را در شبکه مشخص می‌کند. لازم به ذکر است که در این الگوریتم امنیتی، کاربر و سرور به عنوان اصول امنیتی در نظر گرفته می‌شوند.

[3] Cloud Computing
[4] Biometrice Encryption
[5] Kerbros Distribution Cnter

ISSN: 2745-3673
http://www.Rcsj.ir

روش کار الگوریتم کربروس

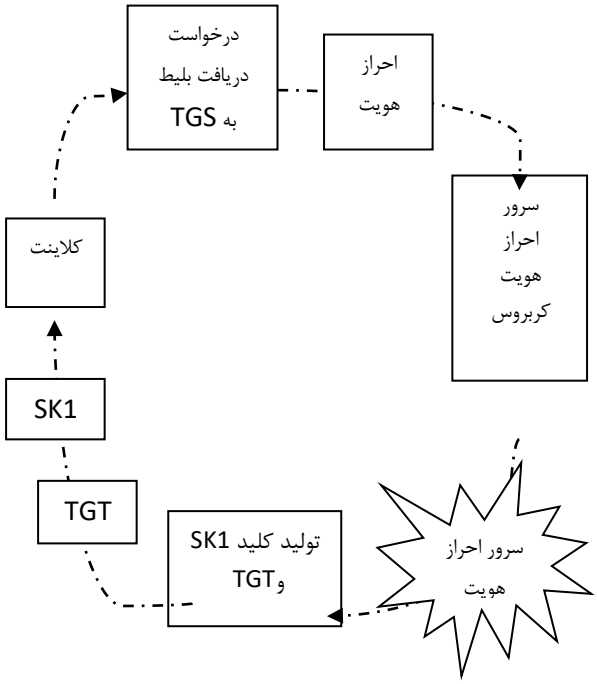
احراز هویت کاربر

بر اساس شیوه عملکرد این الگوریتم، زمانی که یک کاربر قصد ورود به شبکه کربروس را دارد در ابتدا یک پیغام درخواست را که مبتنی بر نام و کلمه عبور خود است را به سمت سرور مربوطه ارسال می‌کند. شبکه نیز اطلاعات مربوط به پیغام ارسالی را که توسط TGT[6] رمزنگاری شده است را دریافت می‌کند. در این راستا الگوریتم کربروس به محض دریافت دریافت TGT، به منظور انجام عملیات رمزگشایی آن از کاربر درخواست می‌کند تا مجدداً کلمه عبور خود را به سمت سرور ارسال کند.

حال چون تنها یک کاربر است که دارای رمز عبور درست است، بنابراین فرآیند مذکور در جهت احراز هویت کاربر عمل می‌کند. پس از تأیید هویت کاربر و رمزگشایی TGT، سرورTGS[7]یک بلیط با عنوان SK1[8] را جهت استفاده کاربر از شبکه صادر می‌کند. شکل (۳) بیانگر روال احراز هویت کاربر می‌باشد (مرحله اول اجرای الگوریتم کربروس).

اجازه دسترسی

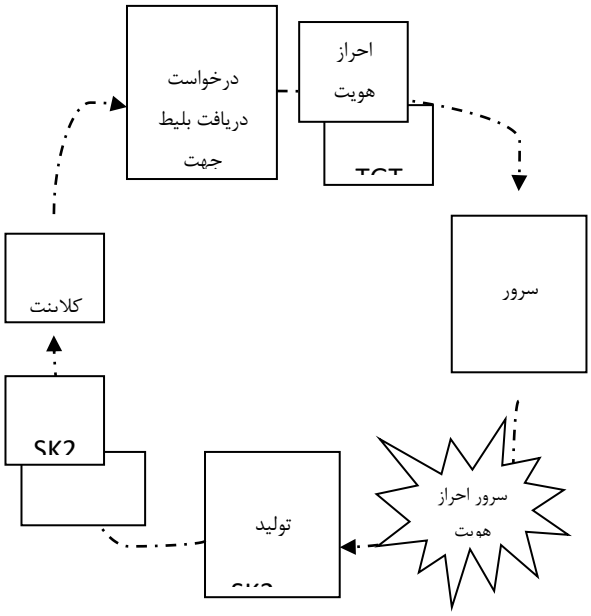
در این مرحله کاربر پس از دریافت پیغام از سرور TGS، آن را رمزگشایی کرده و مقدار کلید SK1 را بدست می‌آورد. سپس کاربر به منظور دریافت اجازه دسترسی یک فایل تصدیق کننده را که شامل نام کاربر، آدرس، تاریخ و زمان فعلی است رامی‌سازد و آن را به همراه TGT به سمت سرور TGS ارسال می‌کند. در ادامه این روال و در سمت شبکه کربروس، متصدی صدور بلیط، فایل‌ها را دریافت می‌کند و آن را رمزگشایی می‌کند. حال اگر مقدار کلید SK1 رمزگشایی شده و اطلاعات موجود در فایل تصدیق کننده معتبر باشد، در این صورت سرور TGS یک کلید جدید به نام SK2[9] را تولید می‌کند و آن را با استفاده از اطلاعات کلید SK1 را به حالت کد درآورده و از آن جهت برقراری ارتباط بین کاربر و سیستم استفاده می‌کند. در نهایت متصدی صدور بلیط، بلیط جدیدی را که شامل نام کاربر، آدرس، تاریخ و زمان، زمان اعتبار و نام کارگزار سیستم است رامی‌سازد و به سمت کاربر می‌فرستند. شکل (۴) بیانگر روال اجازه دسترسی کاربر می‌باشد (مرحله دوم اجرای الگوریتم کربروس).



شکل ۳- ساختار احراز هویت کارب

[6] Ticket Granting Ticket
[7] Ticket Granting Server
[8] Session Key1
[9] Session Key2

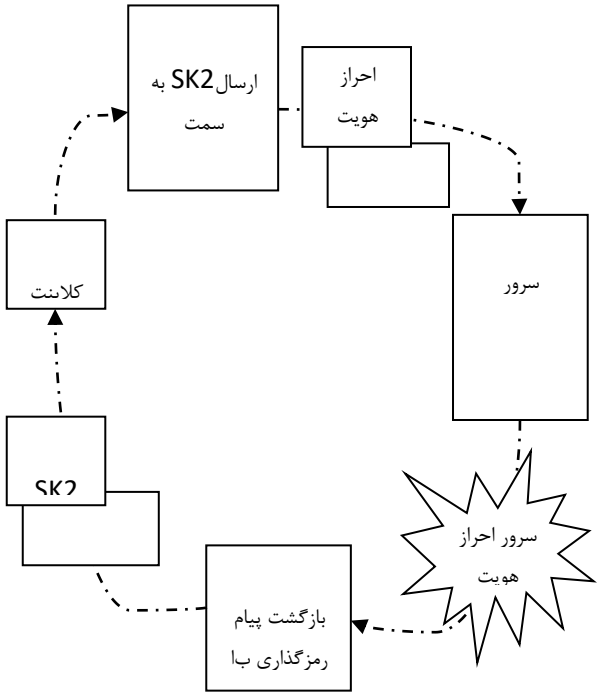
ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۴- ساختار اجازه دسترسی

برقراری ارتباط

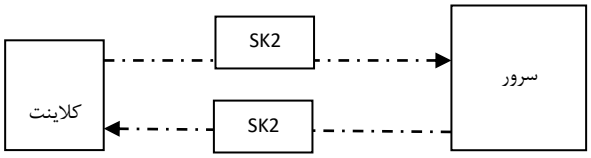
در این مرحله کاربر پس از دریافت بلیط آن را رمزگشایی کرده و مقدار SK2 را بدست می‌آورد. حال به منظور برقراری ارتباط بین کاربر و سیستم، کاربر یک فایل تصدیق کننده جدید را می‌سازد و آن را با استفاده از اطلاعات کلید SK2 را به حالت کد در می‌آورد. سپس کاربر، فایل تصدیق کننده جدید را به همراه بلیطی را که با کلید سیستم رمز کرده است را به سمت سیستم ارسال می‌کند. شکل (۵) بیانگر روال برقراری ارتباط می‌باشد (مرحله سوم اجرای الگوریتم کربروس).



شکل ۵- ساختار برقراری ارتباط

ISSN: 2745-3673
http://www.Rcsj.ir

در ادامه سیستم با دریافت فایل تصدیق کننده (فایلی که با کلید SK2 رمز شده است)، متوجه می‌شود که کاربر واقعی مقدار SK2 را در اختیار دارد. نکته حائز اهمیت این است که زمان و تاریخ قرار گرفته در بلیط، امکان شنود و ذخیره کردن کلید را از هکرها سلب می‌کند. در نتیجه هکرها نمی‌توانند به اطلاعات کلید دسترسی پیدا کنند و از آن در عملیات مخرب استفاده کنند. شکل (۶) بیانگر روال تبادل اطلاعات[10] بین کاربر و سیستم می‌باشد.



شکل ۶- ساختار تبادل اطلاعات بین کاربر و سیستم

ارزیابی مدل پیشنهادی

در این بخش به بررسی نتایج حاصل از شبیه سازی مدل پیشنهادی با مدل‌های رمزنگاری RSA معمولی و اصلاح شده و مدل رمزنگاری AES[11] می‌پردازیم. در ابتدا لازم به ذکر است که الگوریتم کربروس پیشنهاد شده در این پژوهش بر اساس مدل رمزنگاری DES[12] پیاده سازی شده است. از جمله موارد حائز اهمیت در بحث ارزیابی سیستم‌های رمزنگاری می‌توان به طول کلید، شفافیت در تحلیل رمزنگاری، زمان رمزنگاری و رمزگشایی، میزان امنیت و هزینه ذخیره کلید اشاره کرد. از این رو جدول (۱) بیانگر مقایسه اینویژگی‌ها است.

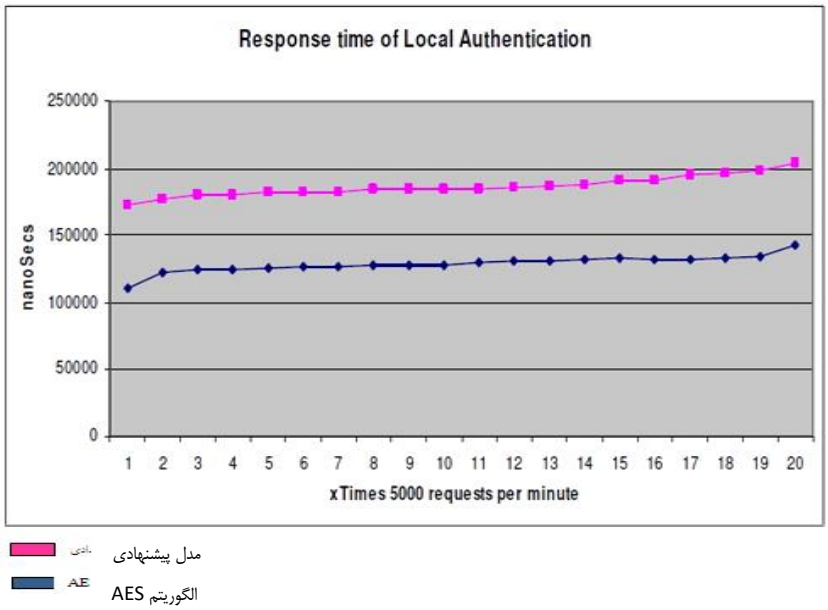
جدول ۱- مقایسه مدل پیشنهادی با مدل‌های رمزنگاری RSA معمولی و اصلاح شده

	مدل پیشنهادی	RSA معمولی	RSA اصلاح شده
طول کلید	۶۴ بیت	۶۴ بیت	۶۴ بیت
شفافیت در تحلیل رمزنگاری	خیر	خیر	بله
زمان رمزنگاری و رمزگشایی	۲.۸۲ میلی ثانیه	۱۰۹.۶۴ میلی ثانیه	۱۰۳.۳۵ میلی ثانیه
میزان امنیت	بالا	بالا	بالا
هزینه ذخیره کلید	کم	زیاد	زیاد

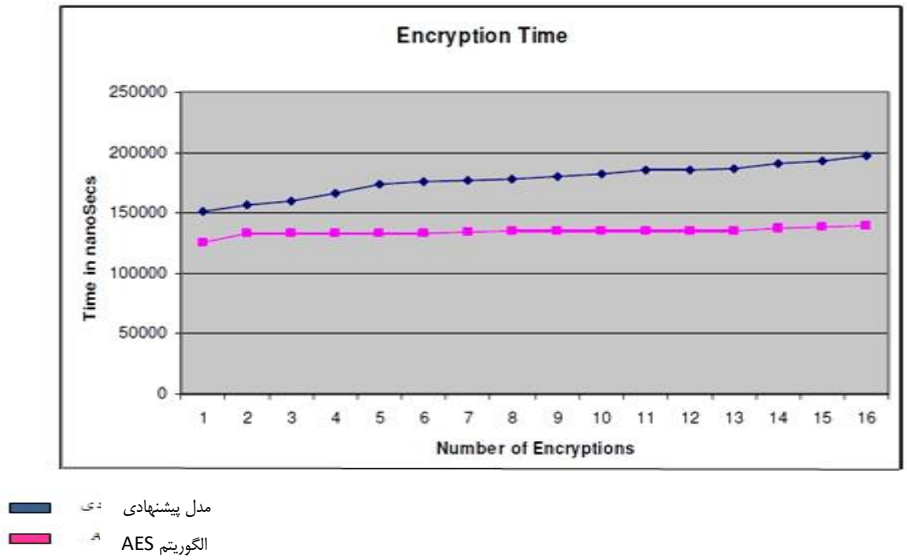
همچنین نمودارهای (۱) و (۲) نیز به ترتیب بیانگر مقایسه زمان پاسخ و زمان رمزنگاری مدل پیشنهادی با الگوریتم AES می باشد.

[10] Information Interchange
[11] Advanced Encryption Standard
[12] Data Encryption Standard

ISSN: 2745-3673
http://www.Rcsj.ir



نمودار ۱-مقایسه زمان پاسخ مدل پیشنهادی با الگوریتم AES



نمودار۲- مقایسه زمان رمزنگاری مدل پیشنهادی با الگوریتم AES

نتیجه گیری

بررسی‌های انجام شده حاکی این موضوع است که مقوله‌های امنیت و حریم خصوصی در وب، با گسترش اینترنت و ابزارهای اطلاع‌رسانی بیش از پیش نادیده گرفته شده‌اند و بدین وسیله حقوق فردی کاربران کمرنگ‌تر از قبل شده است. با توجه به اهمیت حریم خصوصی و تأثیر آن بر تک تک افراد جامعه، نمی‌توان این مسأله را حل نشده باقی گذاشت. از این رو ما در این پژوهش با بکارگیری الگوریتم کربروس که درواقع یک پروتکل امنیتی برای احراز هویت کاربران در شبکه است، سیستم احراز هویتی را که مبتنی بر ۳ اصل احراز اصالت، مجاز شماری و حسابرسی است، ارائه داده‌ایم. نتایج حاصل از شبیه‌سازی این مدل در بخش ارزیابی حاکی از برتری این الگوریتم نسبت به مدل‌های رمزنگاری RSA معمولی و اصلاح شده و مدل AESمی‌باشد.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[۱] حلواچی، ه.، "یک معماری امن سمپاد برای حفظ حریم خصوصی، محرمانگی، و صحت داده"، پایان نامه کارشناسی ارشد، دانشگاه صنعتی شریف، ۱۳۹۲..

[۲] میرمحمدی، ز.، و پورمظفری، س.، "بهبود الگوریتم رمز منحنی های بیضوی با استفاده از کدگذاری داده"، کنفرانس بین المللی رمز ایران، ۱۳۸۹.

[۳] نقیان فشارکی، م.، طباطبایی، س. غ. ح.، و تمتاجی، م.، "ارائه معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمان"، فصلنامه علمی- پژوهشی«امنیت پژوهی»، ص.۹۱- ۱۱۳، ۱۳۹۳.

[4] Chan, J., Bateman, L., and Olafsson, G.," *A people & purpose approach to humanitarian data information security and privacy* ", ELSEVIER, Humanitarian Technology: Science, Systems and Global Impact, Vol. 159, No. 20, 2016.

[5] Dahal, S., *"Security Architecture for Cloud Computing Platform"*, (Master of Science Thesis), Stockholm University, Sweden, 2012.

[6] Goasin, A., and Arora, A., "*Security Issues In Data warehouse: A Systematic Review*", ELSEVIER, International Conference on Intellingent Computing, Communication and Convergence (ICCC), Vol. 48, No. 10, 2015.

[7] Lio, H., Ning, H., Xiong, Q., and Yang, L. T., *" Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing "* , IEEE, pp. 1-11, 2014.

[8] Omar, M. N., Salleh, M., and Bakhtiari, M., (2014), *"Biometric encryption to enhance confidentiality in Cloud computin*", Paper presented at the International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, PP.45-50.

[9] Reshmi, G., and Rakshmy, C. S., *" A Survey of Authentication Methods in Mobile Cloud Computing "* , International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, pp. 58-63, 2015.

[10] Singh, J., and Kang, E. S. S., "*Security Enhancement in WEP by Implementing Elliptic Curve Cryptography Technique*", ELSEVIER, International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, No. 5, 2012.