مطالعات مدیریت و کارآفرینی
دوره ۸، شماره ۳ ، پاییز ۱۴۰۱
صفحات ۲۵-۱۷

Online ISSN: ٢٤٧٦-٤٣٧X
Print ISSN: ٢٥٣٨-٢٠٦٣
www.irijournals.com

امنیت شبکه در مدیریت سازمانی: مفاهیم و کاربردها

عباس رضایی مقدم

کارشناسی ارشد فناوری اطلاعات، شهرداری خرم‌آباد

چکیده

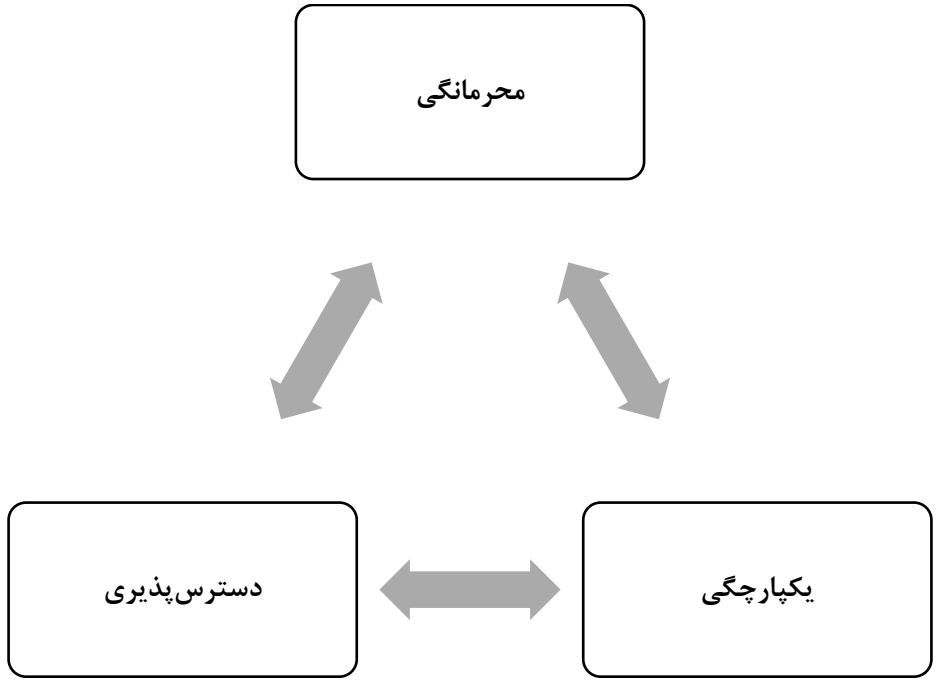
پیچیدگی فزاینده مسائل و مشکلات شهری به‌خصوص در کلان‌شهرها، نیاز آن‌ها را به جامع‌نگری حل این مسائل اجتناب‌ناپذیر نموده است. ازجمله این مسائل هوشمندسازی شهری، تأمین زیرساخت‌های فناوری و تأمین امنیت شبکه آن می‌باشد، ایجاد، تأمین و حفظ امنیت در یک سازمان به مؤلفه‌های مختلفی بستگی دارد و بروز بودن زیرساخت‌های نرم‌افزاری یکی از آن مؤلفه‌هایی است که اهمیت بالایی هم دارد. عموماً به‌روزرسانی زیرساخت‌های نرم‌افزاری نیاز به تخصص خاص و عمیقی ندارد ولی می‌تواند باعث بهبود امنیت و ثبات شبکه و دارایی‌های آی تی شرکت و یا سازمان شود. در راستای موارد مذکور، پژوهش حاضر با هدف، تحلیل مفهوم امنیت شبکه، ضرورت و کاربرد آن تدوین شده است.

واژگان کلیدی: امنیت شبکه، مدیریت شهری، کاربرد، فناوری اطلاعات.

مقدمه

در هر شبکه‌ای تمامی اطلاعات ارسالی و دریافتی برای سازمان مهم هستند .حفاظت از این داده‌ها در بستر شبکه ابتدا نیاز به وجود امنیت در کل شبکه دارد. امنیت شبکه جهت جلوگیری از حملات افراد خارج از سازمان، جلوگیری از ورود آنها به پیکربندی شبکه و سوءاستفاده‌های احتمالی اعمال می‌شود. امر امنیت شبکه با استراتژی‌های مختلف بر جنبه‌های سخت افزاری و نرم‌افزاری اعمال می‌شود تا تهدیدات خارجی مجال تخریب شبکه را نداشته باشند. از آنجایی که تهدیدات و حملات شکل‌های مختلف داشته و بر سطوح مختلف شبکه تأثیرات متفاوت می‌گذارند، تأمین امنیت شبکه هم نیازمند انجام کارهای مختلف است (۱). امروزه پیشرفت استفاده از تکنولوژی های مدرن در مدیریت شهرها، سرعت زیادی یافته است. اما ایران نسبتا از این قاعده مستثنی است و اغلب کلان شهر های آن، با روند کندی به سمت این فناوری ها در حال حرکت هستند و در شهر های کوچک آن، حتی ردی هم از این فناوری ها به چشم نمی خورد (۲). همواره استفاده از انواع فناوری های هوشمند در شهرها، هزینه های گزاف میلیاردی با خودش به همراه دارد، لذا بی تردید باید آسایش بیشتری را برای شهروندان فراهم سازد. فناوری، فناوری است و باید موجب راحتی و آسایش انسانها شود. قطعا همه ی تکنولوژی های جدید و پیشرفته دارای ریسک های جدی و اجتناب ناپذیری هستند. شهرهایی که از زیرساخت های متصل به شبکه برخوردارند، دائما خطر هک شدن آنها را تهدید می کند. این موضوع در زندگی روزمره کاربران هم مشاهده می شود و هر چه قدر دستگاه های متصل به اینترنت افزایش می یابد، میزان امنیت هم با کاهش مواجه می شود. اما مطمئنا هک شدن یک یا دو دستگاه خانگی در برابر هک شدن تمام سیستم مدیریتی یک شهر ، خیلی متفاوت است و این خطری است که می تواند میلیون ها شهروند را تهدید کند (۳).

امنیت دارای سه رکن به شرح شکل زیر است:

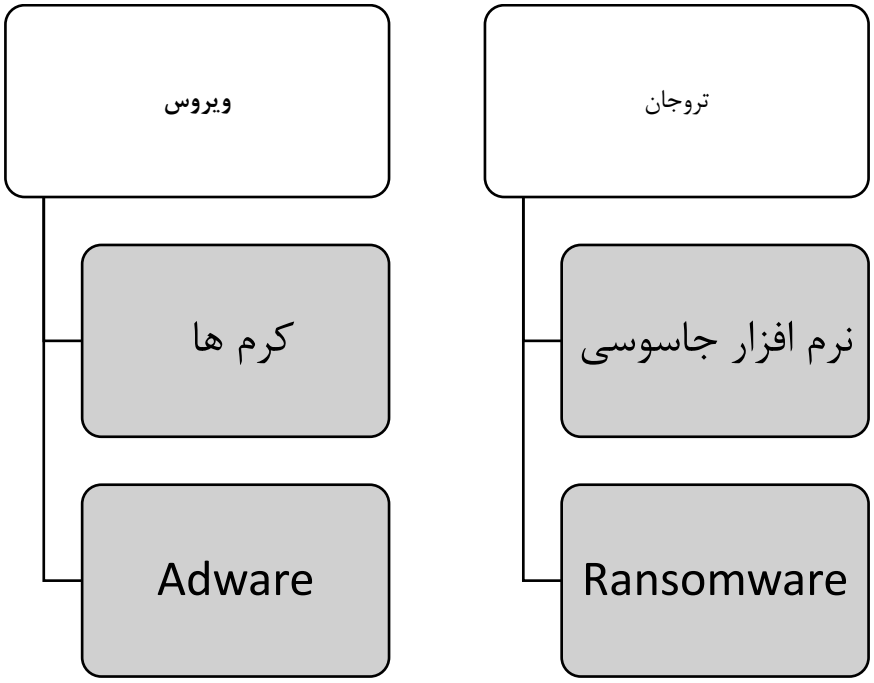


شکل ۱: ارکان امنیت

امنیت شبکه یک پردازش چند لایه است. تعیین نوع و نحوه تلقین لایه های دفاعی مورد نیاز فقط پس از تکمیل ارزیابی قابل ارائه است. تهیه لیستی از سیاست های اجرایی بر مبنای اینکه چه چیزی برای سازمان مهم تر و انجام آن سادتر است در اولویت قراردارد پس از آنکه این اولویت ها به تایید رسیدند هر یک از آن‌ها باید به سرعت در جای خود به اجرا گذارده شود، ارزیابی امنیتی شبکه یک بخش بسیار مهم تر از برنامه ریزی امنیتی است. امنیت شبکه در حالت کلی به مجموعه اقداماتی گفته می شود که به منظور جلوگیری از بروز مشکلات امنیتی در بستر شبکه صورت می گیرد. این مجموعه اقدامات می تواند بصورت راهکارهای متعددی در غالب سرویس های سخت افزاری و نرم‌افزاری پیاده سازی شوند. لازم به ذکر است که معمولا بسیاری از روشهای تأمین امنیت توسط رول ها (Roles) صورت می گیرد.

چه مواردی باعث به خطر افتادن امنیت شبکه می شوند؟

موارد مخرب مختلفی وجود داشته که به شبکه شما آسیب وارد می‌کنند (۴). در ادامه برخی از این موارد عنوان شده‌اند:



شکل ۲: موارد مخرب امنیت شبکه

ویروس: ویروس یک فایل مخرب و قابل دانلود است که می‌تواند در سیستم باقی مانده و با تغییر سایر برنامه‌های رایانه‌ای با کد خاص خود، تکرار شود. هنگامی که ویروس پخش می‌شود، فایل‌ها آلوده شده و می‌توانند از رایانه‌ای به رایانه دیگر منتقل شده و داده های شبکه را خراب یا نابود کنند.

کرم‌ها: می‌تواند با گرفتن پهنای باند و همچنین کاهش کارایی رایانه شما در پردازش داده‌ها، سرعت شبکه را پایین بیاورد. یک کرم یک بدافزار مستقل است که می تواند مستقل از سایر فایل‌ها، جایی که ویروس برای پخش شدن نیاز به برنامه میزبان دارد، پخش و کار کند.

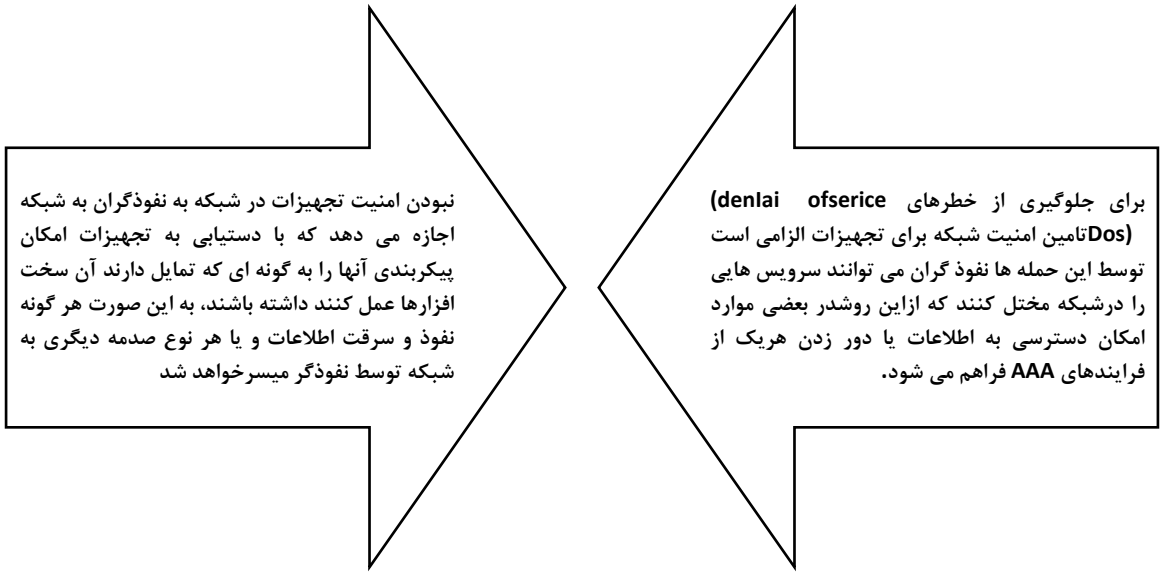
تروجان :یک تروجان یک برنامه مخرب است که شبیه به برنامه‌های کاربردی واقعی به نظر می‌رسد که به سرعت تأثیر منفی بر شبکه می‌گذارد. یک ویروس تروجان می‌تواند فایل‌ها را حذف کرده، سایر بدافزارهای مخفی در شبکه رایانه شما مانند ویروس را فعال کرده و داده‌های ارزشمند را سرقت کند.

نرم افزار جاسوسی: همانند نام خود، یک ویروس رایانه‌ای است که اطلاعات شخص یا سازمانی را بدون اطلاع صریح آن‌ها جمع‌آوری می‌کند و ممکن است اطلاعات جمع آوری شده را بدون رضایت مصرف کننده به شخص ثالث ارسال کند.

Adware: می‌تواند درخواست‌های جستجوی شما را به وب سایت‌های تبلیغاتی هدایت کند و داده‌های بازاریابی مربوط به شما را در این مرحله جمع آوری کند تا تبلیغات سفارشی بر اساس سابقه جستجو و خرید شما نمایش داده شود.

Ransomware: این مورد یک نوع نرم افزار سایبری تروجان است که برای به دست آوردن پول از رایانه شخص یا سازمانی که بر روی آن نصب شده است، داده‌ها را رمزگذاری کرده به گونه‌ای که غیر قابل استفاده بوده و دسترسی به سیستم کاربر را مسدود می‌کند.

الزام امنیت شبکه برای سازمان ها



شکل ۳: الزام امنیت شبکه برای سازمان ها

در سازمان ها و مسلماً شهرداری ها یک کارمند ناراضی ویااخراجی می تواند یک تهدید، بالقوه برای امنیت مجموعه باشد که شاید بتوان با راهکارهای الکترونیکی و فنی شبکه از تبدیل شدن آن به یک جمله یا تهدید بالفعل جلوگیری به عمل آورد. ازجمله راهکارهای امنیت شبکه در شهرداری ها می توان به: وجود یک مدیر روشنفکر و کارا، بالا بردن آگاهی شهرداری در خصوص امنیت فیزیکی شبکه، استفاده از نرم افزارهای آنتی ویروس قوی و نرم افزارهای امنیت اینترنت، استفاده از رمزهای عبور احراز هویت وتعویض ماهانه آن ها و... اشاره نمود (۵).

شبکه شهری

شبکه شهری یا شبکه کلان شهری به انگلیسی (Metropolitan Area Network) :یک شبکه کامپیوتری بزرگ است که معمولاً در سطح یک شهر گسترده می‌شود. در این شبکه‌ها معمولا از زیرساخت بیسیم یا اتصالات تجهیزات فیبر نوری جهت ارتباط محل‌های مختلف استفاده می‌شود.

شبکه شهری MAN چیست؟

استاندارد IEEE 802-2001 شبکه کلان شهری را به صورت زیر تعریف می‌کند: یک شبکه MAN برای ناحیه جغرافیایی بزرگ‌تری از یک شبکه محلی بهینه شده است و از حد چند بلوک ساختمانی تا گستره یک شهر را می‌تواند شامل شود. سرعت شبکه‌های کلان شهری نیز مانند شبکه‌های محلی می‌تواند بسته به کانال‌های ارتباطی از حدود متوسط تا سرعت‌های بالا تغییر کند.

دسترسی در شبکه شهریMAN

در این شبکه امکان دسترسی به یک ابر برای تمام استفاده‌کننده‌ها فراهم می‌گردد، البته نکته قابل تامل این است که باید بستر فیبر نوری با ظرفیت بالا وجود داشته باشد تا نودها در فواصل نزدیک نصب شده و توان تشعشعی پایینی از آنتن‌های بی‌سیم انتشار پیدا کند.

مدیریت یک شبکه شهری

مالکیت و اداره یک شبکه شهری MAN می‌تواند در اختیار یک سازمان باشد، ولی معمولاً سازمان‌ها و افراد بسیاری در این امر نقش ایفا می‌کنند. همچنین ممکن است که شبکه‌های شهری به عنوان خدمات عمومی در اختیار و اداره دولت باشند. این شبکه‌ها اغلب برای اتصال شبکه‌های محلی مختلف به یکدیگر بستر مناسب را ارایه می‌دهند.

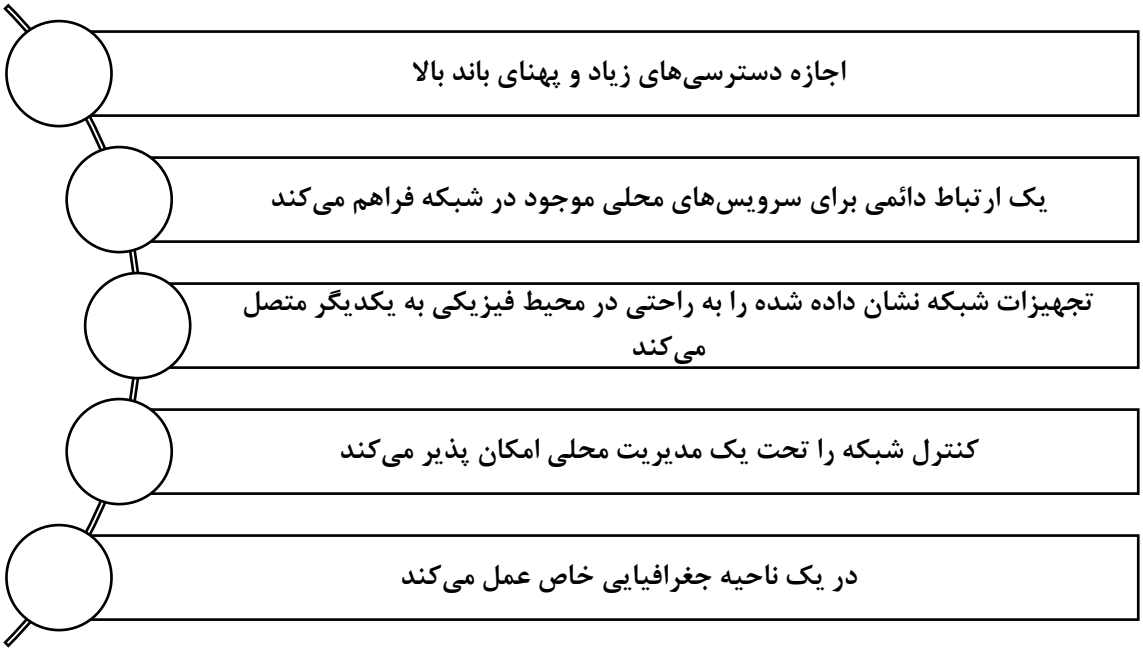
جنبه‌های فنی شبکه شهری

بعضی فناوری‌ها که به این هدف بکار می‌روند عبارتند از حالت انتقال ناهمگام(ATM) ، فناوری اف‌دی‌دی‌آی (FDDI) و SMDS.این فناوری‌های قدیمی‌تر در حال جایگزین شدن با شبکه‌های کلان شهری هستند که براساس اترنت (Ethernet) کار می‌کنند (به عنوان نمونه متروواترنت (Metro Ethernet) که در بسیاری از مناطق پیاده شده است).

شبکه‌های MAN که ارتباطات بین شبکه‌های محلی را بدون نیاز به کابل شبکه فراهم کنند نیز ساخته شده‌اند و از ارتباطات میکروویو(Microwave) ، رادیویی (Radio) یا لیزر مادون قرمز (Infra-red Laser) استفاده می‌کنند.

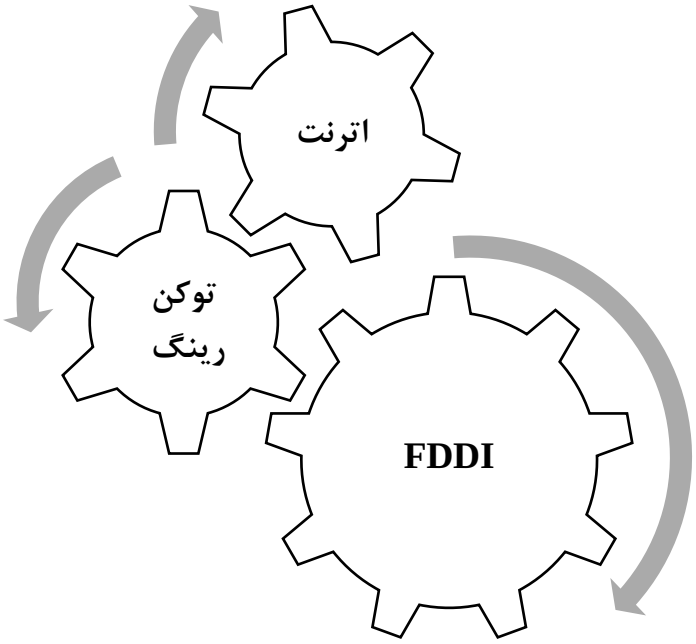
استاندارد DQDB یک استاندارد شبکه کلان شهری برای ارتباطات دیتا است. این استاندارد در استاندارد IEEE 802.6 تعریف شده است. با استفاده از استاندارد DQDB شبکه‌ها می‌توانند تا ۳۰ مایل گسترده شوند و در سرعت‌های بین ۳۴ تا ۱۵۵ Mbit/sعمل کنند.

خصوصیات شبکه شهری MAN



شکل ۴: خصوصیات شبکه شهری MAN

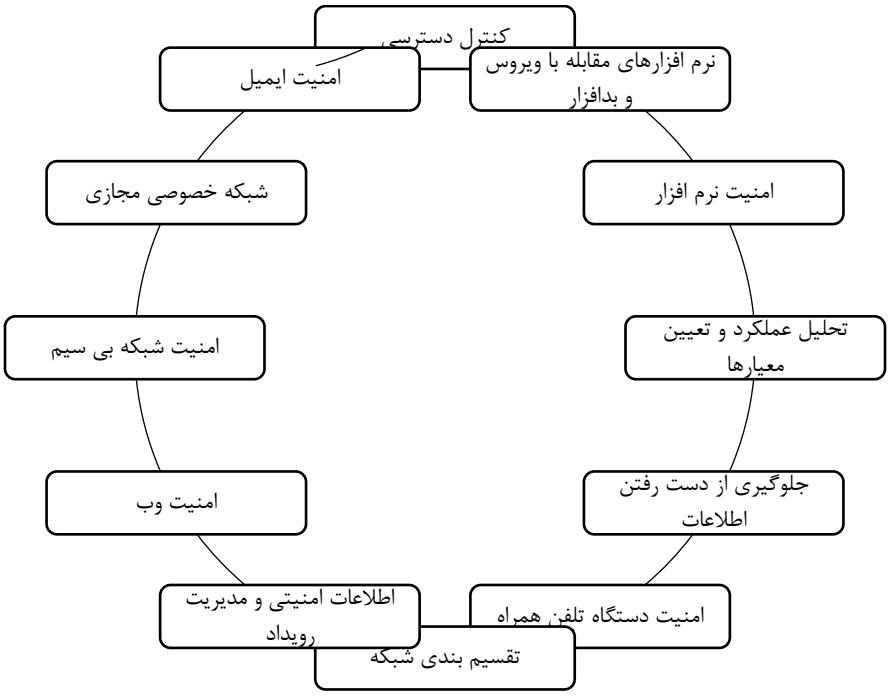
پروتکل‌های موجود در این شبکه



شکل ۵: پروتکل‌های موجود در شبکه شهریMAN

انواع راهکارها در مباحث امنیت شبکه

موارد زیر جزو اساسی ترین مباحث و راهکارهای کنترل امنیت در انواع مقیاس ها است. البته برخی موارد در مقیاس های کوچکتر قابل حذف هستند اما اگر امنیت اهمیت بالایی دارد بهتر است بر روی تمامی موارد زیر کار شود:



شکل ۶: راهکارهای تأمین امنیت شبکه

نتیجه گیری

هوشمندسازی، تأمین هزینه‌های زیرساختی در حوزه فناوری اطلاعات و ایجاد امنیت شبکه و ارتقا زیرساختارهای فناوری اطلاعات در شهرها ضرورتی انکارناپذیر است و می بایستی به این موضوع توجه ویژه ای شود و به عبارتی شهرهای کشور باید به سمت هوشمندسازی و تأمین امنیت شبکه رفته تا از تمامی مزایای آن بهره‌مند شوند در غیر این صورت تنها منجر به تحمیل هزینه فاقد مزیت خواهند شد.

منابع

1. Goldstein, A., Frank, U.: Components of a Multi-perspective Modeling Method for Designing and Managing IT Security Systems. Information Systems and e-Business Management, vol. 14, pp. 101–140. Springer, Berlin (2015)
2. Ahmed, R.K.A.: Overview of security metrics. Softw. Eng. 4(4), 59–64 (2016)
3. Suhartana, M., Pardamean, B., Soewito, B.: Modeling of risk factors in determining network security level. Int. J. Secur. Appl. 8(3), 193–208 (2014)
4. Jouini, M., Rabai, L.B.A., Aissa, A.B.: Classification of security threats in information systems. Procedia Comput. Sci. 32, 489–496 (2014)

۵. محرم زاد، هما (۱۳۹۷)، نقش امنیت شبکه وضرورت اجرای آن در سازمانهای مردم نهاد (مطالعه موردی شهرداری ها)، همایش بین المللی افق های نوین در مهندسی کامپیوتر و فناوری اطلاعات.