پژوهش در مهندسی عمران و معماری ایران ، شماره ۱۷، تابستان ۱۳۹۹، ص ۶۶- ۵۰

ISSN: 2475-3673
http://www.Racj.ir

مجله علمی پژوهش در علوم رایانه (سال پنجم)
شماره ۱۸ / تابستان ۱۳۹۹ / ص ۶۶- ۵۰

بهبود امنیت در اینترنت اشیاء بر اساس الگوریتم آشوبناک

فائزه رضائی ملاسرائی[۱]، مسعود طالب ضیابری[۲]، احمد باقری[۳]

[۱] دانشجوی کارشناسی ارشد؛ موسسه اموزشی عالی احرار رشت.

[۲] استاد راهنما؛ موسسه اموزشی عالی احرار رشت.

[۳] استاد مشاور؛ دانشگاه گیلان.

نام نویسنده مسئول:
فائزه رضائی ملاسرائی

تاریخ دریافت: ۱۳۹۹/۳/۱
تاریخ پذیرش: ۱۳۹۹/۵/۸

چکیده

با توسعه مداوم فناوری اطلاعات در عصر حاضر فناوری رایانه تبدیل به یک رسانه مهم برای انتقال اطلاعات در زندگی مردم شده است و اینترنت اشیا منجر به پیشرفت سریع فناوری‌هایی مانند ادراک داده‌ها، انتقال داده های بی‌سیم و پردازش اطلاعات هوشمند شده است. با افزایش میزان انتقال اطلاعات در کنار مسائلی همچون سرعت و کیفیت باید به امنیت اطلاعات نیز توجه فراوانی شود. که در این راستا از پروتکل SMT (پروتکل انتقال پیام ایمن) برای انتقال کلید استفاده می شود در این مقاله تلاش شده است که با استفاده از الگوریتم آشوبناک کلیدی با حساسیت بالا و شبه تصادفی تولید شود تا با استفاده از ان اطلاعات رمز نگاری شده و کلید از طریق پروتکل MODSMT (انتقال پیام ایمن اصلاح شده) به گیرنده انتقال می یابد تا با استفاده از ان اطلاعات رمزنگاری شده تنها توسط گیرنده قابل بازگشایی باشند.

واژگان کلیدی: اینترنت اشیاء، مدل هرج و مرج، امنیت اینترنت اشیاء، رمزنگاری کلید، الگوریتم.

پژوهش در مهندسی عمران و معماری ایران ، شماره ۱۷، تابستان ۱۳۹۹، ص ۶۶- ۵۰
ISSN: 2475-3673
http://www.Racj.ir

مقدمه

با پیشترفت مداوم فناوری های رایانه، امروزه پیام رسان های رایانه ای به یک رسانه مهم برای انتقال اطلاعات در زندگی روزانه مردم تبدیل شده اند. همان طور که برقراری این ارتباط میان مردم بسیار زندگی انها را بهبود می بخشد اما خطرات پنهان امنیت اطلاعات نیز بوجود می اید که باید این خطرات از بین بروند.در این راستا مکانیزم انتقال داده ها با استفاده از مسیریابی چند مسیری می تواند به طور موثری امنیت انتقال داده را بهبود ببخشد.با این حال از لحاظ دسترسی و محرمانگی امنیت این پروتکول های پیام چندرسانه ای دارای معایبی هستند. پروتکل SMT در راستای مبادله کلید قابل استفاده نیست بنابراین محرمانه بودن ان ضعیف اس. پروتکل SDM (اطمینان از مسیریابی چند منظوره مبتنی بر داده ها) عملکرد بهتری دارد از این رو که اگر یک قطعه داده در حین انتقال از دست رفته باشد،گره مقصد نمی تواند پیام اصلی را به دست اورد. این مقاله در راستای مقاله پیشین زکر شده در منبع به دنبال بهبود کلید تولید شده در زمان واقعی می باشد[7].

امنیت شبکه کامپیوتر بر اساس محافظت از محیط داخلی شبکه ، عمدتا برای محافظت از نرم‌افزار و اطلاعات هارد دیسک در سیستم شبکه کامپیوتری است.با ارائه یک طرح حفاظتی موثر، عملکرد منظم خدمات شبکه های کامپیوتری را می توان تضمین نمود.

تکنیک های بهینه سازی داده شبکه بی سیم مشترک و تکنیک های امنیتی اطلاعات به شرح زیر است:

۱-انتخاب بزرگترین واحد انتقال. اندازه بزرگترین واحد انتقال به طور مستقیم تعیین می کند که زمان لازم برای حمل بسته در طول ارتباطات شبکه باشد. در یک شبکه بی سیم، اندازه بزرگترین واحد انتقال باید با دقت انتخاب شود. اگر واحد حداکثر انتقال بیش از حد بزرگ باشد، نسبت داده های معتبر بسته بسیار بزرگ است، که باعث از بین رفتن منابع پهنای باند شدید است که قبلا بسیار محدود است.

۲-متراکم سازی داده ها. اگر میزان خطای بیت یکسان باشد، بین مقدار داده منتقل شده و احتمال وقوع میزان خطای بیت رابطه ای متناسب وجود دارد. فشرده سازی داده ها موجب صرفه جویی در پهنای باند و همچنین احتمال اشتباهات در نرخ انتقال را کاهش می دهد. فشرده سازی داده ها دو جنبه فشرده سازی را شامل می شود، یعنی فشرده سازی بارهای بسته و فشرده سازی هدر بسته.

۳-بهینه سازی پروتکل کنترل انتقال در محیط بی سیم، دلیل از دست دادن بسته های داده ها این است که علاوه بر تراکم شبکه، در اغلب موارد، TCP مکانیسم کنترل احتمالی را به نحوی اشتباه باز کرده است. این باعث می شود سرعت انتقال کاهش یابد، که در نهایت منجر به کاهش عملکرد آن خواهد شد. علاوه بر این، در طول انتقال ارتباطات سلولی، سیستم اشتباه باعث کنترل تراکم TCP می شود.

۴-نوآوری ها و پیشرفت های پروتکل های دیتاگرام کاربر. در برخی موارد، میزان تلفات بسته های UDP در یک محیط بی سیم ممکن است بیش از ۵۰٪ باشد. دلیل این امر عمدتا به دلیل سیگنال پیوند بی نهایت و تضعیف BER بالا است.

۵-M-UDP به منظور آشنایی کامل شدن پدیده تضعیف سیگنال بی سیم، M-UDP تمام داده های ارسال شده به میزبان را با کپی کردن آن بر میزبان نظارت می کند. پس از انهدام سیگنال پیوند بی نهایت، میزبان منتقل می شود و میزبان نظارت کننده تمام داده های قبلا کپی شده را دوباره ارسال می کند. در طول فرایند انتقال داده ها، تمام داده های جدید به طور خاص در میزبان نظارت کننده ذخیره می شوند.

در یک شبکه ارتباطات، هر پروتکل از یک هدر استفاده می کند که نشانی ها، شماره های توالی، بیت های پرچم، شاخص های طول و غیره را حمل می کند و بیت های CRC ممکن است برای تشخیص خطا اضافه شوند. پروتکل SMT امکان انتقال داده ها را فراهم می کند، که یک انتقال داده با چندین مسیر با تکنولوژی انبساط است. گره مقصد می تواند داده های اصلی را هنگامی که بخشی از قطعه داده را دریافت می کند داده اصلی را بازیابی کند و پروتکل را می توان به طور مستقیم به پروتکل مسیریابی اساسی پیوند داد. فرض بر این است که پروتکل SMT ارتباط امنیتی بین گره های منبع و مقصد برقرار می کند، SMT می تواند قابلیت اطمینان هر مسیر را با بطور پیوسته اندازه گیری انتقال و پذیرش موفقیت آمیز بسته ها در آن مسیر ها را برآورد کند. الگوریتم SMT به طور کلی از الگوریتم توزیع داده استفاده می کند و مبنای نظری الگوریتم الگوریتم Rabin

ISSN: 2475-3673
http://www.Racj.ir

است. اساس اصلی الگوریتم Rabin رمزگذاری پاک است، که اطلاعات اضافی را به داده ها اضافه می کند تا گیرنده بتواند داده های اشتباه را در صورت خطاهای داده ای خاص تعمیر کند.

اینترنت اشیاء

چهارچوب اینترنت اشیاء

امروزه ترقی جامعه را نمی‌توان از پیشرفت فناوری اطلاعات جدا نمود. با توسعه فناوری اطلاعات، جهان تغییرات بزرگی را تجربه کرده است و زندگی انسان بهبود یافته است. در سیستم صنعت اطلاعات، اینترنت اشیائ یکی از مهمترین نکات رشد است. اینترنت اشیاء جهانی را توصیف می کند، که در آن هر چیزی، از جمله اشیاء بی جان، برای خود دارای هویت دیجیتال می باشند و به کامپیوترهای دیگر اجازه می دهند آنها را سازماندهی و مدیریت کنند و موجب هوشمندتر شدن اشیاء گردند. و به این ترتیب وظایف مانند شناسایی هوشمند و مدیریت در قالب یک شبکه را تکمیل می کند. معماری شبکه ای که اینترنت اشیا را تشکیل می دهد شامل یک لایه حسگر، یک لایه شبکه و یک لایه کاربردی است. در لایه حسگر، فناوری حساسیت و تکنولوژی کسب اطلاعات برای درک و شناسایی دنیای فیزیکی استفاده می شود. در لایه شبکه، انتقال و جایگزینی اطلاعات با استفاده از تکنولوژی اینترنت اشیائ برای ارتباط با شبکه ها و شبکه های ارتباطی تکمیل می شود. در لایه کاربردی، نرم افزار الگوریتم حرفه ای و نرم افزار محاسبه برای تکمیل پردازش، محاسبه و ادغام اطلاعات مورد استفاده قرار می گیرند.

ارتباط در اینترنت اشیاء

مهم ترین بخش در اینترنت اشیاء را می توان برقراری ارتباط میان اشیاء بیان نمود، که از طریق برچسب الکترونیکی هدف و شبکه حسگر تحقق می یابد. RFID یک فناوری برچسب الکترونیکی اصلی در فرایند توسعه IOT می باشد.

تکنولوژی RFID با توجه به انعطاف پذیری و کاربردهای بسیار، برای خودکارسازی شناسایی اشیاء بسیارمناسب می باشدRFID . یک تکنولوژی پیامرسانی بدون تماس است.RFID از سیگنال های فرکانس رادیویی برای انجام کار مربوطه استفاده می کند و از قابلیت های تجزیه و تحلیل اطلاعات برای شناسایی اطلاعات شیء استفاده می کند. سیستم RFID از سه بخش اصلی تشکیل شده است: خوانندگان، آنتن ها و برچسب های الکترونیکی.

نحوه عملکرد RFID در اینترنت اشیا بدین‌صورت است که اطلاعات مربوط به شیء که به آن برچسب الصاق شده است کدگذاری می‌شود. به هنگام هر ورود و خروج اشیا از مکان‌های مهم کنترلی یک خوانندگان کدهای موجود در برچسب‌ها که بر روی اشیا هستند را می‌خوانند، سپس خوانندگان اطلاعات خوانده شده را برای پایگاه داده ارسال می‌کنند. در این سرورها از اطلاعات دریافتی URL مربوط به سرور مقصد تشخیص داده می‌شود و با آن اتصال ایجاد می‌نماید. در این حالت هر زمان که این برچسب خوانده شود، اطلاعات آن از طریق اینترنت برای مبدأ اصلی آن شی منتقل می‌شود. بدین ترتیب تمام اعضای مرتبط در جریان تمامی اطلاعات قرار می‌گیرند ..نقش آنتن برای دریافت و ارسال سیگنال های داده است. به طور کلی موقعیت آنتن در برچسب الکترونیکی یا خواننده قرار خواهد گرفت.

لایه های IOT و نیازمندی های امنیتی اینترنت اشیاء

IOT به طور کلی به چهار لایه اصلی تقسیم می شود که عبارت اند از:

- لایه کربرد: این لایه از برنامه‌ها و سرویس‌های مختلفی که IoT ارائه می‌دهد، تشکیل شده است.برنامه‌ها و کاربردها شامل شهرهای هوشمند، خانه‌های هوشمند ، حمل و نقل ، امکاناتو مراقبت‌های بهداشتی می‌شوند.مانند: شهرهای هوشمند – لوازم هوشمند – حمل و نقل هوشمند – حمل و نقل هوشمند.
- لایه دریافت: این لایه از انواع مختلف تکنولوژی‌های حسی از جمله حسگرهایدما، حسگرهای ارتعاش، حسگرهای فشار و حسگرهای RFID تشکیل شده است که به دستگاهاجازه می‌دهند سایر اشیاء را حس کند.مانند: گره های حسگر حسگر های RFIDدروازه حسگر.

ISSN: 2475-3673
http://www.Racj.ir

●لایه شبکه: این لایه از نرم‌افزار ارتباطات شبکه و همچنین اجزای فیزیکیمانند توپولوژی، سرورها، گره‌های شبکه و اجزای شبکه که امکان ارتباط شبکه را فراهممی‌آورند، تشکیل شده است. هدف اصلی آن انتقال داده‌ها میان دستگاه‌ها و از دستگاه‌هابه گیرنده‌ها می‌باشد.مانند: اینترنت -محاسبه ی ابر – شبکه های ارتباط سیار.

●لایه فیزیکی: لایه فیزیکی شامل سخت‌افزار پایه مانند اجزای فیزیکی، لوازمهوشمند و تجهیزات برقی که به عنوان پایه و اساس شبکه‌بندی اشیاء هوشمند عمل می‌کنند،تشکیل شده است.مانند: اجزای فیزیکی -تجهیزات برقی -قفل و امنیت فیزیکی.

کاربران می توانند از طریق پلت فرم مدیریت به شبکه وارد شوند تا اطلاعات مرتبط را مشاهده کنند. مثلا یک شهر هوشمند (اینترنت چیزها) را بیابید: سازمانی یا کاربر هویت دستگاه ترمینال از طریق پلت فرم اینترنت اذعان می کند تا اطمینان حاصل شود که دستگاه واجد شرایط در نهایت به طور معمول در پایانه های کاربر مورد استفاده قرار می گیرد. ساختن پلت فرم صدور گواهینامه امنیت اینترنت به طور عمده مطالب زیر را شامل می شود.

۱) ساختار زیر ساخت های امنیتی عمدتا شامل سیستم مدیریت کلید، دستگاه سخت افزاری رمزنگاری و مرکز تأیید اعتبار است. این عمدتا مسئول مدیریت، توزیع و لغو تراشه کلیدی یا کلید رمزنگاری کاربر است. زیرساخت های امنیتی پایه و اساس کل پلت فرم صدور گواهینامه امنیتی IoT است.

۲) ساخت یک پلت فرم پشتیبانی ایمنی. یک دستگاه تأیید هویت دستگاه بر اساس کلیدهای متقارن ساخته شده است. سیستم تأیید هویت مسئول تأیید اعتبار سنجی دستگاه لایه حسگر و هویت کاربر لایه کاربرد است. در عین حال، در سطح درک، سیستم تأیید هویت نیز مسئول بازخورد موقتی و صحیح و اطلاع از وضعیت دستگاه است.

۳) ساخت یک سیستم تأیید هویت و مجوز کاربر. سیستم تأیید هویت و مجوز عمدتا شامل یک ماژول تأیید هویت کاربر، یک ماژول تک نشانه گذاری و یک ماژول مدیریت مجوز است. ماژول تأیید اعتبار هویت کاربر مسئول پیاده سازی یکپارچه تأیید هویت است که یک حالت اعتبارسنجی کلیدی امن بر اساس یک کلید رمزنگاری فراهم می کند. ماژول تک نشانه یک حالت plug-and-play را فراهم می کند. کاربر فقط باید برای تأیید هویت هویت یکبار برای ورود به لیست سرویس های مختلف برنامه با توجه به کنترل و مدیریت ماژول مجوز، نیاز به انجام اصلاحیه سیستم پس زمینه داشته باشد. ماژول مدیریت مجوز یک تابع کنترل دسترسی مبتنی بر نقش را فراهم می کند، یعنی پس از اینکه کاربر تأیید هویت را منتقل می کند، کاربر با توجه به نقش کاربر به حقوق مختلف اعطا می شود، بنابراین اجرای تابع کنترل دسترسی برای کاربر اجرا می شود.

۴) سیستم امضا دیجیتال بر اساس کلید متقارن. سیستم امضای دیجیتال مسئولیت اعطای دیجیتالی دستگاه سنسور لایه حسگر و اطلاعات داده شده توسط کاربر لایه کاربردی را برای تأیید اطمینان از انتقال اطلاعات و اطمینان از صحت و منحصر به فرد دستگاه حسگر مسئولیت میدهد.

۵) سیستم انتقال رمزگذاری داده. سیستم انتقال رمزگذاری داده ها عمدتا تابع رمزگذاری اطلاعات یا فایل ها را در طول انتقال اینترنت اشیائ انجام می دهد. مهمترین مسئله در فرآیند رمزگذاری و رمزگشایی، مشکل اصلی است. سیستم امنیتی داده ها مکانیسم مبتنی بر کلید متقارن را به طور کامل متعهد به اطمینان از سرعت و کارایی رمزنگاری و رمزگشایی می کند و امنیت بر اساس مکانیسم امنیتی سطح تراشه همچنین امنیت کلید را تضمین می کند.

۶) سیستم حسابرسی امنیتی یک رکورد کامل رفتار دستگاه یا کاربر را فراهم می کند. مدیر سیستم می تواند به طور مستقیم از عملکرد سیستم و دسترسی به دستگاه حسگر یا کاربر نگه داشته شود.

۷) سرویس تأیید هویت دستگاه (DAS) خدمات احراز هویت را برای دستگاه های حسگر فراهم می کند و مدیران سیستم می توانند به صورت اختیاری خدمات احراز هویت را پیکربندی کنند.

۸) سرویس تأیید هویت و مجوز کاربری، تأیید هویت کاربر و مدیریت حقوق را فراهم می کند. مدیران سیستم می توانند ارتباط بین کاربران، نقش ها و مدیریت حقوق را پیکربندی کنند، در نهایت کاربران با یک پلت فرم نرم افزار راحت و امن را ارائه می دهند.

پلت فرم صدور گواهینامه IoT پشتیبانی جامع فنی از جمله سیستم های تست محیطی نرم افزار، استقرار در محل، نصب سیستم، و عیب یابی در طول فرایندهای سیستم و نگهداری سیستم را فراهم می کند.

ISSN: 2475-3673
http://www.Racj.ir

از آنجا که دستگاه های آگاه IoT-aware در محیط های نظارت نشده مستقر هستند، آنها به مسائل امنیتی مختلف آسیب پذیر هستند. یک روش احراز هویت دو طرفه می تواند بین دستگاه حسگر و سرور برای حل مشکل دسترسی ترمینال اعتماد آگاه و دسترسی به سرور مورد اعتماد استفاده شود. فرآیند خاص به شرح زیر است:

۱) سنسور یک درخواست احراز هویت را آغاز می کند و پارامتر زمانبندی را به تراشه رمزگذاری منتقل می کند.
۲) تراشه رمزگذاری یک کد تأیید اعتبار را با توجه به پروتکل احراز هویت تولید می کند.
۳) سنسور کد اعتبارسنجی را به مرکز داده منتقل می کند.
۴) پس از دریافت کد احراز هویت، مرکز داده آنرا به سرور احراز هویت ارسال می کند.
۵) سرور احراز هویت کد تأیید اعتبار ورودی را تایید می کند و نتیجه تأیید هویت را به مرکز داده بازگرداند.

در پروژه IoT فعلی، طرف سرور به طور تصادفی ارتقاء و انجام وظایف مرتبط مانند کار روزانه را انجام می دهد. پس از اینکه دستگاه گره هویت سرور را تأیید می کند، دستورالعمل مربوطه را اجرا می کند تا مانع از دریافت دستگاه کنترل حسابی شود. بنابراین، دستگاه سنجش نیاز به تایید هویت سرور دارد. سرور هنگام ارسال فرمان خود کد احراز هویت خود را تولید می کند و دستگاه حسگر کد تأیید اعتبار دریافتی را تأیید می کند. اگر احراز هویت ناموفق باشد، سرور جعل هویت می کند و فرمانی که آن را منتقل می کند اعتبار ندارد. از سوی دیگر، اگر احراز هویت تصویب شود، دستگاه سنجش بر اساس دستور سرور دریافت شده اجرا می شود.

امنیت پروتکل انتقال داده پیشرفته: MODSMT

پروتکل MODSMT فرمت پروتکل SMT است که از مکانیزم های امنیتی متعددی برای اطمینان از محرمانه بودن داده ها استفاده می کند. مکانیزم های امنیتی عبارتند از یک سازنده کلید تولید بر اساس عملکرد یک طرفه از ارزش مخفی، یک مکانیزم مبادله کلید چند D-H بر اساس چند مسیری، یک روش انتقال که در آن داده های رمز شده و پارامتر های مربوطه کلید جدا شده است.

کلید جلسه بین گره منبع و گره مقصد در پروتکل MODSMT به صورت پویا با استفاده از یک عملکرد یک طرفه محاسبه می شود و مقدار مخفی باید مبادله شود. روش های متعدد مبادله کلید با استفاده از پروتکل MODSMT برای پیاده سازی مبادله ارزش مخفی می باشند.

فرض کنید که مسیر داده ها در پروتکل مسیریابی چند مسیریابی به عنوان {p1,p2,….,pn} نشان داده شده است.

$$S \to D: \{g^{xS} mod\, p_i \parallel T_{sI} \parallel E_{SK_S}(g^{xS} mod p_i \parallel T_{sI})\} \quad (۱)$$

جایی که Tsl تایمر است؛SKS کلید است؛ و (فرمول ۱) نشان دهنده داده های رمز شده است. پس از دریافت پیام، گره مقصد D، هویت پیام را با کلید عمومی گره منبع S بررسی می کند و پیام را به گره S از طریق مسیر قابلیت اطمینانزیرمجموعه باز می گرداند.

$$D \to S: \{g^{yx} mod p_i \parallel T_{DI} \parallel E_{SK_D}(g^{xS} mod p_i \parallel T_{DI})\} \quad (۲)$$

گره منبع S شناسه پیام بازگشت را با کلید عمومی گره مقصد D بررسی می کند.

$$S_{SD} = g^{xSyD} mod\, min(p_i . p_j) \quad (۳)$$

در MODSMT، کلیدهای جلسه با استفاده از یک عملکرد یک طرفه (به عنوان fsS مشخص می شود) بر اساس مقادیر مخفی.

فرایندهایی که توسط گره منبع S ارسال داده می شوند به شرح زیر می باشند:

$$C_k = E_{fsS.D_{(nk)}}(m_i \parallel seq \parallel k \parallel T) \quad (۴)$$

ISSN: 2475-3673
http://www.Racj.ir

با استفاده از تابع هش، ما داریم:

$$H_k = h(m_i \parallel seq \parallel k \parallel T) \quad (۵)$$

برای بهبود امنیت انتقال، پارامترهای تصادفی مورد استفاده برای محاسبه کلید و پیام رمزگذاری شده از طریق همان مسیر انتقال نمی یابند. داده های ارسالی در مسیر به شرح زیر است:

$$s \underset{p_k}{\rightarrow} D: \{h(C_k \parallel H_k \parallel n_{k-1} \quad (۶)$$

مدل سه درجه ازادی هرج و مرج در ایجاد کلید

شبکه هرج و مرج

در دهه های اخیر یافته شده است که پدیده های هرج و مرج در مغز وجود دارد. به عنوان یک پدیده جالب بسیار غیر خطی ، هرج و مرج به طور جدی در جوامع ریاضیات ، علوم و مهندسی مورد بررسی قرار گرفته است. تئوری هرج و مرج می تواند برخی از فعالیت های نامنظم را در مغز انسان توضیح دهد. بنابراین، پویایی هرج و مرج فرصت جدیدی برای مردم برای مطالعه شبکه های عصبی فراهم می کند. مدل هرج و مرج دارای نقطه تعادل ثروتمندتر است که نه تنها شامل جذب کننده های نقطه ثابت و جذب کننده های نقطه ای است، بلکه جذب های عجیب و غریب نیز دارد. با توجه به انباشت اثرات خود مراقبتی مدل هرج و مرج ویژگی آن می تواند یک روش جستجوی اکتشافی باشد.

به همین خاطر با استفاده از روش های رمزنگاری توالی ساده ی سه درجه ازادی هرج و مرج این مقاله یک کلید خارجی را برای رمزگذاری سیستم معرفی می کند.

تولید کلید

به منظور استفاده از توالی تصادفی تولید شده توسط شبکه های هرج و مرج به رمز گذاری داده ها، در این مقاله از سیستم خودمختار سه بعدی ساده زیر استفاده شده است:

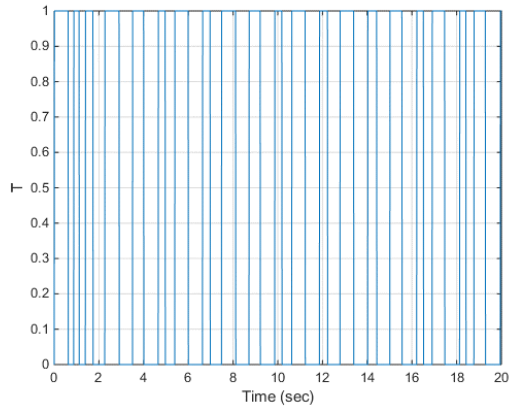
$$\begin{cases} x = y - ax + byz \\ y = cy - xz + z \\ z = dxy - hz \end{cases} \quad (۷)$$

که در آن $[x(t) \quad y(t) \quad z(t)]^T \in R^3$ بردار حالت است و a، b، c، d و h ثابت های واقعی مثبت هستند.

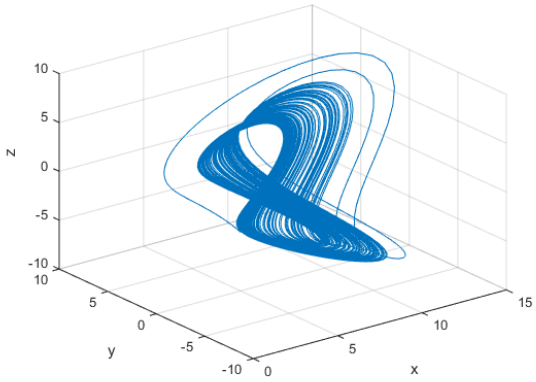
این سیستم جدید در طیف وسیعی از پارامترها آشفته است و دارای رفتارهای پیچیده جالب بسیاری است. به عنوان مثال، سیستم می تواند برای پارامترهای $a = 3$، $b = 2.7$، $c = 4.7$، $d = 2$، $h = 9$ و شرایط اولیه $[۵ ، ۰ ، -۴]^T$ جذب جدید هرج و مرج جدید ایجاد کند.

مطابق با تابع فرمول (۷) میزان (۰،۱) های تولید شده در بازه زمانی بیست ثانیه به صورت نمودار دو بعدی را در شکل (۱) مشاهده می کنید. در شکل (۲) نمودار فضای سه بعدی (x,y,z) را مشاهده می نمایید.شکل (۳) نشان دهنده نمودار دو بعدی (x,y) می باشد، شکل (۴) نشان دهنده نمودار دو بعدی (x,z) می باشد، شکل (۵) نمایش دهنده نمودار دو بعدی (z,y) بوده و شکل (۶) نمودار دو بعدی (x,y,z) را در یک نمودار واحد نمایش می دهد. بیشترین میزان هرج و مرج در بازه زمانی تعیین شده مقایص بردار های [x(t),y(t),z(t)] نشان داده شده است.

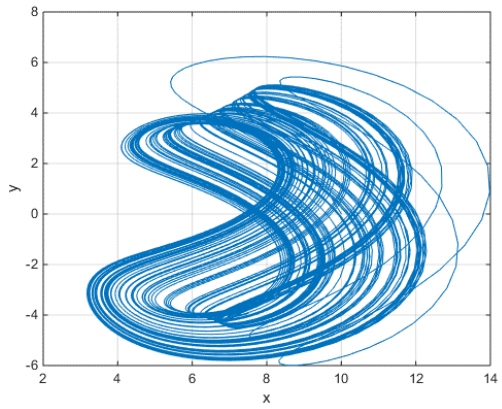
ISSN: 2475-3673
http://www.Racj.ir



شکل(۱):میزان(۰،۱) تولید شده در بیست ثانیه

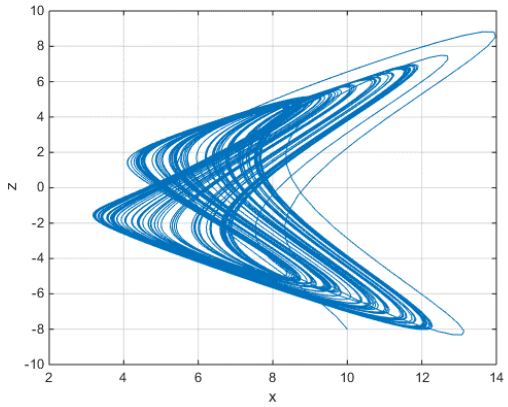


شکل(۲):نمودار فضای سه بعدی(x,y,z)

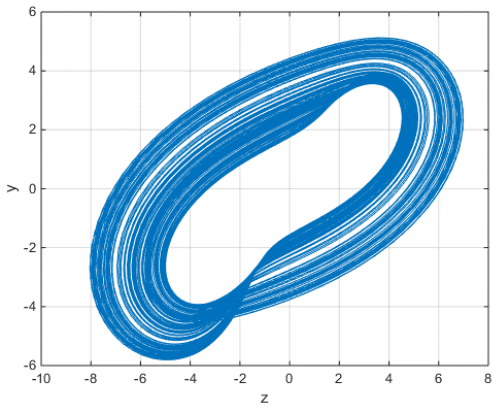


شکل(۳):نمودار دو بعدی(x,y)

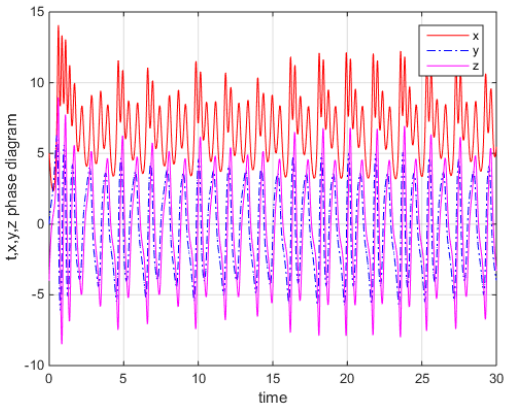
ISSN: 2475-3673
http://www.Racj.ir



شکل(۴):نمودار دو بعدی(x,z)



شکل(۵):نمودار دو بعدی(z,y)



شکل(۶):نمودار دو بعدی(x,y,z)

تولید کلید باینری

در این مقاله برای ایجاد کلید و رمز نگاری داده ها ابتدا باید کلید تولید شده به صورت باینری در آید که در این راستا از یک شرط برای تولید باینری ها به صورت تبدیل تمام مقیاص های به دست امده کوچک تر از صفر به (0) و تمام مقیاص های بزرگ تر از صفر به (1) ، استفاده شده است.

$$f(x)\begin{cases}1 & x>0\\ 0 & x<0\end{cases}$$

ISSN: 2475-3673
http://www.Racj.ir

همان طور که مشاهده می کنید صفر و یک ها با استفاده از یک حلقه به تعداد ماتریکس ایجاد شده از فایل مورد رمز نگاری ،تولید شده اند.

رمز نگاری

این مقاله با استفاده از نرم افزار MATLAB پیاده سازی شده است که در این بخش چگونگی رمزنگاری یک پیام متنی مورد ازمون و خطا قرار گرفته است. تابع استفاده شده برای رمز نگاری تابع بولی XOR می باشد، در این تابع بول اگر همه متغیرهای ورودی از یک نوع باشند یعنی اگر همه ورودی‌ها یک یا صفر باشد خروجی صفر خواهد بود.در غیر این صورت برابر یک می‌باشد.

۱. در رمزنگاری این بخش ابتدا داده ای متنی با سه نوع متفاوت (کاملا فارسی-کاملا انگلیسی-فارسی و انگلیسی)به صورت جداگانه به برنامه داده می شود، سپس داده های وارد شده به زبان انسان برای رمزنگاری به صورت باینری در می آیند.که در جدول(۱) مشاهده می کنید.

جدول(۱):داده های باینری شده.

Binary			
نوع جمله	پست الکترونیک به نامه دیجیتالی می گویند	Email is called digital mail	نمونه ای از پست های الکترونیک عبارتند از:Gmail،Email
صفر و یک ها وسطر و ستون های جمله تبدیل شده به باینری	11001111110 11000110011 11000101010 00000100000 11000100111 11001000100 11010101001 11000101010 11000110001 11001001000 11001000110 11001001010 11010101001 00000100000 11000101000 11001000111 00000100000 11001000110 11000100111 11001000101 11001000111 00000100000 11000101111 11001001010 11000101100 11001001010 11000101010 11000100111 11001000100	1000101 1101101 1100001 1101001 1101100 0100000 1101001 1110011 0100000 1100011 1100001 1101100 1101100 1100101 1100100 0100000 1100100 1101001 1100111 1101001 1110100 1100001 1101100 0100000 1101101 1100001 1101001 1101100	11001000110 11001000101 11001001000 11001000110 11001000111 00000100000 11000100111 11001001010 00000100000 11000100111 11000110010 00000100000 11001111110 11000110011 11000101010 00000100000 11001000111 11000100111 11000100111 11001000100 11010101001 11000101010 11000110001 11001001000 11001000110 11001001010 11010101001 00000100000 11000111001

ISSN: 2475-3673
http://www.Racj.ir

11000101000 11000100111 11000110001 11000101010 11001000110 11000101111 00000100000 11000100111 11000110010 00000111010 00001100101 00001101101 00001100001 00001101001 00001101100 11000001100 00001100111 00001101101 00001100001 00001101001 00001101100		11001001010 00000100000 11001000101 11001001010 00000100000 11010101111 11001001000 11001001010 11001000110 11000101111	

۲. سپس با استفاده از الگوریتم توضیح داده شده در بخش(۲,۳) کلیدی تولید شده که برای رمز نگاری با داده های باینری با استفاده از روش بخش (۲,۴) به صورت باینری در امده از دیگر خصوصیات کلید تولید شده این است که این کلید دارای تعداد یکسانی با داده ی ورودی می باشد. جدول(۲).

جدول(۲):تولید کلید

key			
نمونه ای از پست های الکترونیک عبارتند از:Gmail،Email	Email is called digital mail	پست الکترونیک به نامه دیجیتالی می گویند	نوع جمله
01001000111	01001000111	01001000111	صفر و یک ها وسطر و ستون های کلید تولید شده
11100010111	11100010111	11100010111	
10000000000	10000000000	10000000000	
11111111101	11111111101	11111111101	
01111110101	01111110101	01111110101	
00000000111	00000000111	00000000111	
11111000000	11111000000	11111000000	
00111110111	00111110111	00111110111	
10001111111	10001111111	10001111111	
11000000101	11000000101	11000000101	
11111110100	11111110100	11111110100	
01010111100	01010111100	01010111100	
00010000000	00010000000	00010000000	
11111110010	11111110010	11111110010	
00000001100	00000001100	00000001100	
00000101111	00000101111	00000101111	
10000000000	10000000000	10000000000	

ISSN: 2475-3673
http://www.Racj.ir

01111111000 00000011111 11111100000 10110011111 11111001000 00001111111 11111010000 01010111111 11010000000 01000111110 10100000000 00000000111 11110111100 00111110100 00000001111 11111001000 00000010111 10000000000 00011111110 11110001111 11111110010 00000111111 11000000000 11111111010 00001010111 10000000000 00000000011 11111101000 00000011111 10111100000 01111111100 00000000010 10001000000	011111110	01111111000 00000011111 11111100000 10110011111 11111001000 00001111111 11111010000 01010111111 11010000000 01000111110 10100000000 00000000111 11110111100 00111110100 00000001111 11111001000 00000010111 10000000000 00011111110 11110001111 11111110010 00000111111	

۳. پس از تولید کلید برای رمز نگاری داده ی باینری شده و کلید را با استفاده از تابع XOR رمز نگاری می نماییم که در این مرحله داده به دست امده داده ای است که اگر به زبان انسان باز گردانی شود و نمایش یابد برای زهن انسان غیرقابل درک می باشد جدول(۳).

جدول(۳):داده های رمز نگاری شده.

Encrypted			
نوع جمله	پست الکترونیک به نامه دیجیتالی می گویند	Email is called digital mail	نمونه ای از پست های الکترونیک عبارتند از:Gmail،Email
صفر و یک ها وسطر و ستون های داده‌ی رمزنگاری شده	10000111001 00100100100 01000101010 11111011101 10111010010	11000011010 01011010100 00100111011 11101111110 00110001100	10000000001 00101010010 01001001000 00110111011 10110110010

ISSN: 2475-3673
http://www.Racj.ir

00000100111	10100000001	11001000011	
00111100111	11000100001	00101101001	
11110111101	11100111010	11111011101	
10001011111	00010110100	01001001110	
00000100010	01010001101	00001001101	
00111000110	11001100111	00110110010	
01010011100	00011001111	10011110110	
11011111110	11111001111	11000101001	
00111000001	10110010011	11111010010	
11000100110	11011001000	11000100100	
00000001111	00011110100	11001101000	
01001000111	00000111010	10000100000	
10111011111	000010010	10110111110	
11000111000		11000111000	
00110100100		00110100101	
01100110110		01111011000	
00111100010		11111101000	
11001001110		11001010000	
00110011000		00110011010	
10011111001		10010010011	
00011001010		00011001010	
10010010111		10000010100	
10100100000		01100100111	
11000111110		11001000011	
00110010100		00111110110	
11111010011		00111010100	
11000111110		11001001010	
00111100010		00110000010	
11001010001		00000110111	
01000101111		01010101111	
00011011110		11010110110	
00110101000		00111000101	
00111000000		00110110100	
00000000101		11000010000	
11001100101			
11110010111			
00000110110			
10001101001			
00001101111			
00111100100			
00001111000			
10110001101			
01110011101			
00001101011			
10000101100			

پژوهش در مهندسی عمران و معماری ایران ، شماره ۱۷، تابستان ۱۳۹۹، ص ۶۶- ۵۰

ISSN: 2475-3673
http://www.Racj.ir

۴. در این بخش کلید تولید شده در بخش قبل به همراه داده ی رمز نگاری شده از طریق پروتوکل مورد نظر در اینترنت اشیاء به گیرنده ارسال می شود و برای بازگشایی پیام رمز نگاری شده در کامپیوتر گیرنده پیام رمز شده با کلید دریافت شده با استفاده از تابع XOR رمزگشایی می گردد. تا ماتریکس اولیه پیام به دست آید جدول(۴).

جدول(۴):داده های رمز گشایی شده.

Unencrypted			
نوع جمله	پست الکترونیک به نامه دیجیتالی می گویند	Email is called digital mail	نمونه ای از پست های الکترونیک عبارتند از:Gmail.Email
صفر و یک ها وسطر و ستون های دادهی رمزگشایی شده	11001111110 11000110011 11000101010 00000100000 11000100111 11001000100 11010101001 11000101010 11000110001 11001001000 11001000110 11001001010 11010101001 00000100000 11000101000 11001000111 00000100000 11001000110 11000100111 11001000101 11001000111 00000100000 11000101111 11001001010 11000101100 11001001010 11000101010 11000100111 11001000100 11001001010 00000100000 11001000101 11001001010 00000100000 11010101111 11001001000 11001001010 11001000110 11000101111	10001011101 10111000011 10100111011 00010000011 01001111001 10100000110 00111100001 11011001101 10011001011 10010001000 00110010011 01001110011 11101001111 01001100001 11011000100 00011011011 10000111010 011101100	11001000110 11001000101 11001001000 11001000110 11001000111 00000100000 11000100111 11001001010 00000100000 11000100111 11000110010 00000100000 11001111110 11000110011 11000101010 00000100000 11001000111 11000100111 11000100111 11001000100 11010101001 11000101010 11000110001 11001001000 11001000110 11001001010 11010101001 00000100000 11000111001 11000101000 11000100111 11000110001 11000101010 11001000110 11000101111 00000100000 11000100111 11000110010 00000111010

ISSN: 2475-3673
http://www.Racj.ir

00001100101 00001101101 00001100001			

در انتها برای نمایش پیام به صورت قابل درک برای انسان ماتریکس پیام که بصورت باینری می باشد به متن تبدیل می شود.

۵. آزمایش دیگری که انجام گرفت ازمایش هک شدن یا استفاده از کلید مشابه در روی داده رمزنگاری شده بود. که در این بخش الگوریتم رمز نگاری کلید دوچار تغییر های تصادفی در سطر و ستون های متفاوت شد تا میزان تغییر پاسخ نهایی با ایجاد کوچکترین تغییر در کلید بررسی شود که باعث شد نتیجه نهایی به طور کامل غیر قابل تشخیص با جواب صحیح به دست امده با استفاده از کلید اصلی شود. جدول(۵).

همان طور که در جداول بالا مشاهده می کنید در این مقاله داده ها برای بررسی حجم و زمان اجرا به سه روش متفاوت وارد شده اند که در وش اول تمامی داده های ورودی به زبان فارسی می باشند در این بخش همان طور که در جدول(۶) مشاهده می کنید داده ها در ۱۱ سطر و ۳۹ ستون قرار می گیرند و در مجموع ۴۲۹ داده باینری را در بر می گیرند. در روش دوم تمامی داده های ورودی به زبان انگلیسی می باشند که پس از تبدیل به باینری در یک ماتریکس ۷ سطر و ۲۸ ستونه قرار گرفته اند که ۱۹۶ داده ی باینری را در بر می گیرد. در دو بخش بالا به وضوح تفاوت بین داده های فارسی و انگلیسی قابل مشاهده می باشد که داده های فارسی دارای حجم بالا تری بوده و ماتریکس بزرگتری را ارائه می دهند که زمان اجرای ان نیز بیشتر از زمان اجرای داده ی کاملا انگلیسی می باشد.

در روش سوم داده ها به صورت ترکیبی از دو زبان بالا وارد شده اند که این امر باعث شده است داده ها در ماتریسی با ۱۱ سطر و ۵۰ ستون قرار بگیرند که در کلا ۵۵۰ داده باینری را در بر دارند در این بخش داده های انگلیسی حجم کمتری داشته امابرای قرار گیری در یک ماتریکس واحد به همراه داده های فراسی حجم انها افزایش یافته و با داده های حجیم تر متعادل شده اند. در این بخش زمان اجرا متناسب با حجم داده افزایش یافته است.

ISSN: 2475-3673
http://www.Racj.ir

جدول(۵):آزمون هک کلید.

عنوان	رمزگشایی شده اشتباه	رمزگشایی شده اصلی	کلید اشتباه	کلید اصلی
داده باینری	11100111100 01010100000 00100111100 11110011000 00100100100 01110111001 11110100000 00101000000 00110001001 10001011001 11010001001 01010110110 10000111100 11101010010 10101100000 10001011111 11011011011 101001000	10001011101 10111000011 10100111011 00010000011 01001111001 10100000110 00111100001 11011001101 10011001011 10010001000 00110010011 01001110011 11101001111 01001100001 11011000100 00011011011 10000111010 011101100	00100100110 00001110100 00000000111 00011100110 00010101000 11010111000 00110000001 11001111010 00100111101 11011010100 00011101110 01001111001 01111110011 01011000001 01110101000 10010101011 11011100001 101011010	1000101 1101101 1100001 1101001 1101100 0100000 1101001 1110011 0100000 1100011 1100001 1101100 1101100 1100101 1100100 0100000 1100100 1101001 1100111 1101001 1110100 1100001 1101100 0100000 1101101 1100001 1101001 1101100
جواب به دست امده	ocJl@g|Fsz=}^Rg qMy	called Email is digital mail		

جدول(۶):حجم داده های تولید شده در هر نمونه.

نوع جمله	بخش	اندازه		تعداد صفرها	تعداد یک ها
		سطر	ستون		
پست الکترونیک به نامه دجیتالی می_ گویند	binary	۱۱	۳۹	۰	۴۲۹
	key	۱	۴۲۹	۲۱۴	۲۱۵
	Encrypt	۱	۴۲۹	۲۰۵	۲۲۴
	unencrypted	۱	۴۲۹	۲۴۵	۱۸۴
	Result	۱	۳۹	۰	۳۹
Email is called	binary	۷	۲۸	۰	۱۹۶

ISSN: 2475-3673
http://www.Racj.ir

digital mail	key	۱	۱۹۶	۹۹	۹۷
	Encrypt	۱	۱۹۶	۱۰۰	۹۶
	unencrypted	۱	۱۹۶	۹۹	۹۷
	Result	۰	۲۸	۰	۲۸
نمونه ای از پست های الکترونیک عبارتند از: Gmail،Email	binary	۱۱	۵۰	۰	۵۵۰
	key	۱	۵۵۰	۲۸۸	۲۶۲
	Encrypt	۱	۵۵۰	۲۸۶	۲۶۴
	unencrypted	۱	۵۵۰	۳۲۲	۲۲۸
	Result	۱	۵۰	۰	۵۰

نتیجه گیری

با پیشرفت سریع فناوری اطلاعات امروزه رسانه های اجتماعی دارای نقش بسزایی در انتقال اطلاعات در زندگی مردم می باشد.اما با افزایش استفاده از شبکه های رایانه ای همچون اینترنت اشیاء اهمیت مسائل امنیتی انتقال اطلاعات ظاهر می شود. این مقاله با استفاده از شبکه ی آشوبناک یک کلید با میزان حساسیت بالا تولید می شود، که با استفاده از پروتکل MODSMT ذکر شده در مقاله به طور قابل توجهی میزان امنیت رمزنگاری را بهبود می بخشد. از این رو می توان نتیجه گرفت سیستم پویای آشوبناک دارای ویژگی های شبه تصادفی بوده و می تواند به خوبی برای رمز نگاری اطلاعات استفاده شود.اگر چه در انتقال داده ها با نیاز های زمان واقعی بسیار دشوار می باشد برای مثال این رمز نگاری نه تنها اندازه متفاوتی برای پیام های متنی در نظر می گیرد که باعث تفاوت در زمان انتقال پیام ها با زبان های متفاوت می شود برای انتقال داده های تصویری و ویدئویی در زمان واقعی نیز دشوار می باشد.

ISSN: 2475-3673
http://www.Racj.ir

منابع و مراجع

[1] Deng, L., Li, D., Cai, Z., & Hong, L. (2019). Smart IOT information transmission and security optimization model based on chaotic neural computing. Neural Computing and Applications, 1-14.

[2] Wang N, Gao X, Tao D, Yang H, Li X (2018) Facial feature point detection: a comprehensive survey. Neurocomputing275:50–65.

[3] Ghorai G, Pal M (2018) A note on ‘‘Regular bipolar fuzzy graphs’’ Neural Computing and Applications 21 (1) (2012) 197–205. Neural Compute Apply 30(5):1569–1572.

[4] Qiu Y, Bi Y, Li Y, Wang H (2018) High resolution remote sensing image denoising algorithm based on sparse representation and adaptive dictionary learning. In Computational vision and bio inspired computing. Springer, Cham, pp 892–901

[5] Wang N, Gao X, Li J (2018) Random sampling for fast face sketch synthesis. Pattern Recogn 76:215–227

[6] Dadras S, Momeni H.R(2009) A novel three-dimensional autonomous chaotic system generating two, three and four-scroll attractors. doi:10.1016/j.physleta.2009.07.088

[7] Faezeh Rezaee, Dr Masode Taleb Ziabari, Dr Ahmad Bagheri (2019), Encrypting information using the chaotic model in IOT,http/:csc2019.guilan.ac.ir

[8] Niu Z, Hua G, Wang L, Gao X (2018) Knowledge-based topic model for unsupervised object discovery and localization. IEEE Trans Image Process 27(1):50–63

[9] Y. A. Liu, Q. Yu, S. G. Hu, G. C. Qiao, and Y. Liu(2019) A memristor-based transient chaotic neural network model and its application. https://doi.org/10.1063/1.5115540

[10] L.Salim, B.Stelios (2019) Cryptocurrency forecasting with deep learning chaotic neural networks.

[11] https://doi.org/10.1016/j.chaos.2018.11.014

[12] C.Stergiou, K.E. Psannis, B-Gyu.Kim, B.Gupta (2016) Secure integration of IoT and Cloud Computing.http://dx.doi.org/10.1016/j.future.2016.11.031