دوفصلنامه محاسبات و سامانه‌های توزیع شده
www.jdcs.ir

یک روش مبتنی بر رمزنگاری متقارن در احراز هویت برای سیستم های اینترنت اشیا

فرشاد اسدپور

دانشکده مهندسی و علوم پایه، دانشگاه آزاد اسلامی واحد آشتیان، اراک *

چکیده

امروزه استفاده از اینترنت اشیا در دنیای فن آوری اطلاعات نقش پر رنگی دارد و نوع‌های مختلفی از این شبکه در حال استفاده شده هستند. با توجه به اهمیت امنیت در اینترنت اشیا، در این مقاله روشی جهت حفظ امنیت اطلاعات مبتنی بر احراز هویت به کمک رمزنگاری و امضای دیجیتال و همچنین شکست فایل به بخش های کوچکتر ارائه شده است. آزمایشات بر اساس تعداد مختلف بسته های انتقالی برای روش پیشنهادی نشان می‌دهد که این روش به دلیل استفاده از رمزنگاری تصادفی باعث شده است که معیار عملکرد خوبی به ازای بسته های مختلف از نظر معیارهای نظیر مصرف انرژی، دقت و... داشته باشد. همچنین بر اساس روش پیشنهادی ضمن احراز هویت کاربران، سرویس محرمانگی و صحت اطلاعات نیز به نحوی مناسب در روش پیشنهادی مورد توجه قرار گرفته شده است..

کلمات کلیدی: رمزنگاری ، احزار هویت ،اینترنت اشیا، امنیت

Providing a security mechanism for character recognition in objects internet based on cryptography

Farshad Asadpour

Islamic Azad university, Ashtian, Iran

Abstract

Nowadays, Objects internet in the world of information technology has an important role and use in various types. Considering the importance of security in object Internet, this paper presents a way to maintain the security of identity-based information through cryptography and digital signatures file division to smaller sections. Experiments based on the number of transfer packs for the proposed method show that this method, due to the use of random cryptography, has led to a good performance criterion for various packages such as energy consumption, precision, and so on. Moreover, based on the proposed method, user confidentiality and identity the information are also considered appropriately.

تاریخچه مقاله:

تاریخ ارسال:۹۷/۳/۱

تاریخ اصلاحات:۹۷/۵/۱

تاریخ پذیرش:۹۷/۵/۷

تاریخ انتشار:**۹۷/۵/۱۵**

Keywords:

Cryptography
Objects
Internet and Security
internet of thing

روش ارجاع به مقاله:

ف.اسدپور، یک روش مبتنی بر رمزنگاری متقارن در احراز هویت برای سیستم های اینترنت اشیا، دوفصلنامه محاسبات و سامانه های توزیع شده، سال اول، شماره اول، ص ۱۰۹-۱۱۷، سال انتشار ۱۳۹۷.

* فرشاد اسدپور : asadpoor.f@gmail.com

۱ – مقدمه

اینترنت اشیاء [۲]مفهومی جدید در دنیای فناوری اطلاعات و ارتباطات است که در آن هر شیء قابلیت ارسال و دریافت داده از طریق شبکه های ارتباطی، اعم از اینترنت یا اینترانت (شبکه های داخلی) فراهم می شود. در اینجا منظور از شیء انسان، حیوان یا اشیاء در محیط زندگی است. اینترنت اشیاء در واقع به ارتباط اشیاء مختلف از طریق اینترنت و برقراری ارتباط با یکدگیر است و هدف از این ارتباط فراهم کردن تجربه کاراتر و هوشمندتر در زندگی انسان است. اینترنت اشیاء نیز همانند دیگر فناوری‌های جدید و نوظهور در ابتدا مفهومی سردرگم کننده به نظر می رسد [۱].

اینترنت اشیاء یک مبحث تحقیقاتی جدید در بستر اینترنت و شبکه است که نسخه پیشرفته ارتباط ماشین به ماشین است و در آن اشیاء با یکدیگر بدون مداخله انسان ارتباط برقرار می کنند [۱]. با وجود برنامه های کابردی زمان واقعی ارائه شده در IoT، ارتباطات M2M [۳] از نظر فنی و تکنیکی شامل چالش های مختلفی همانند معماری ارتباطات، مصرف بهینه انرژی، مقرون به صرفه بودن، قابلیت اطمینان، حریم خصوصی، سازگاری، امنیت و غیره است [۱].

در چندین سال اخیر با پیشرفت تکنولوژی، مفهوم جدیدی تحت عنوان سیستم های RFID [۴] پدید آمده است. سیستم های شناسایی با استفاده از فرکانس رادیویی، یکی از پرکاربردترین فناوری های شناسایی خودکار می باشند که داده ها را از دستگاه های دور بازیابی و ذخیره می‌کند. این تکنولوژی جهت شناسایی بی سیم داده های ذخیره شده در ریزتراشه برچسب از طریق امواج رادیویی می باشد [۱]. سیستم های RFID کارکرد یکسانی مشابه بارکد فراهم می‌کنند با این تفاوت که بر خلاف بارکدها، امکان خواندن و نوشتن برچسب ها در هر زاویه ای و از میان اشیاء امکان پذیر است و نیاز به خط مستقیم بین برچسب و برچسب خوان نمی باشد [۲].

برچسب خوان می تواند اطلاعات شناسایی شده را از طریق ارتباطات فرکانس رادیویی با برد کم، به دست آورد. به عبارتی برچسب خوان ها داده ها را به برچسب ها ارسال و یا از آنها دریافت می کنند و جز اتصالی برچسب ها و پایگاه داده ها هستند. برچسب خوان، اطلاعات شناسایی شده را به پایگاه داده منتقل کرده و پایگاه داده اطلاعات شناسایی شده را که درون تگ هاست مدیریت می کند [۵].

احراز هویت به فرآیندی گفته می شود که در آن ارسال کننده یا دریافت کننده اطلاعات برای همدیگر اطلاعاتی را ارائه می کنند تا مطمئن شوند آنها همانی هستند که ادعا می کنند. به نوعی در احراز هویت بررسی می شود که شخص یا ... همانی هست که ادعا می‌کند. اگر ارسال کننده یا دریافت کننده اطلاعات نتوانند به درستی برای همدیگر احراز هویت شوند در این میان اعتمادی ایجاد نمی شود که آنها بتوانند با همدیگر تبادل اطلاعات داشته باشند. احراز هویت همانطور که گفتیم یک فرآیند است و این فرآیند هم می تواند بسیار ساده باشد و هم می تواند بسیار پیچیده و دشوار باشد. ساده ترین راهکار احراز هویت که همگی ما از آن استفاده کرده‌ایم ساختار بسیار

[2] Internet Of Things
[3] Machine to machine
[4] radio frequency identification

ساده ، یک کلید احراز هویت متنی است که ما آن را به عنوان پسورد یا رمز عبور می شناسیم و برای احراز هویت شدن در سیستم های مختلف از آن استفاده می کنیم. اما احراز هویت به تنهایی شامل فاکتورهای مختلفی است که برای بالا بردن سطح امنیتی باید آنها را رعایت کرد.[۸]

۲ – پیشینه پژوهش

از یک دیدگاه اقدامات متقابل علیه تهدیدات امنیتی سیستم های RFID را می توان به دوگروه تقسیم کرد: یک گروه مبنی بر الگوریتم های رمزنگاری هستند و گروه دیگر بر اساس الگوریتم های غیر رمز نگاری می باشند. توابع Hash جز طرح های رمز نگاری می باشند [۹] که عملکرد خلاصه ای از پیام هایی که نقش مهمی در احراز هویت پیام ، جامعیت داده ها و امضاهای دیجیتال ایفا می کنند، ارائه می دهد. استفاده از توابع Hash برای پروتکل های امنیت و حفظ حریم خصوصی سیستم های RFID، محبوبیت زیادی یافته است . از آنجایی که ارتباط بین برچسب و برچسب خوان در یک محیط باز از طریق سیگنال های رادیویی اتفاق می افتد مکانیزمی برای اعتبارسنجی و شناسایی پیام ها در هر دو طرف نیاز است که احراز هویت نام دارد [۱۰].

مقاله [۱۱] یک طرح ساده و مقیاس پذیر با قیمت پایین که مبتنی بر عملیات Hash می باشد را برای حل مسائل امنیتی و حفظ حریم خصوصی پیشنهاد کرده است که پروتکل SRFID نام دارد . این طرح، یک احراز هویت متقابل دو گامه بین پایگاه داده و برچسب فراهم کرده و نیاز به یک کانال امن بین برچسب خوان و پایگاه داده برای تکمیل فرایند احراز هویت ندارد. پایگاه داده همه اطلاعات مرتبط با برچسب ها را ذخیره می کند.

نویسندگان در مقاله [۱۲]یک پروتکل احراز هویت متقابل مبتنی بر Hash را به عنوان راه حلی برای مسائل حریم خصوصی و جعل داده پیشنهاد کرده اند. این پروتکل برای ارسال یک مقدار تصادفی تولید شده به وسیله برچسب به پایگاه داده ، بدون افشا، طراحی شده است . هم چنن در این پروتکل ، مقدار تصادفی با یک مقدار سری و پنهانی جایگزین شده و در یک پیغام پاسخ به کار گرفته می شود. ویژگی پروتکل پیشنهادی، تولید ثابت پیغام های پاسخ مشخص بدون واسط هایی از درخواست های تولید شده مورد انتظار توسط دشمن است. این پروتکل در برابر حملاتی چون استراق سمع، ارسال مجدد، تکثیر تگ، جعل داده ، MITM [۵]و به ویژه حمله تجزیه و تحلیل ترافیک و نفوذ سریع ، امن است .

در منبع [۱۶] یک پروتکل ارتباطی برای سیستم‌های RFID در اینترنت اشیا پیشنهاد شده است که امنیت در آن به وسیله اوراکل تصادفی مهیا میشود. در این مدل اشیا دارای یک EPC [۶]منحصر بفرد هستند روش پیشنهادی نیز SPAP نام دارد. این روش از رمز نگاری متقارن و تابع Hasg یکطرفه و XOR استفاده می‌کند. این روش اعتبار سنجی دوطرفه و امنیت داخلی را برقرار کرده و در برابر برخی حملات پایه نیز مقاومت می کند.

[5] man-in-the-middle attack
[6] Engineering, Procurement and Construction

در منبع [۱۷] روش اعتبارسنجی مبتنی بر ABC را برای ادراک اینترنت اشیا پیشنهاد کرده اند.در این معماری کاربر به عنوان ناظر لایه ادراک است و برای دستگاههایی مانند تلفن همراه و کامپیوترهای هوشمند می باشد. در این روش کارایی بهتری را روی گره های حسگر به نسبت مابقی پروتکل ها داشته ایم.

در منبع [۱۸] از دو پروتکل HAC و RAC استفاده کرده اند و در این روش دسترسی به تگ را با استفاده از تابع Hash یکطرفه با قفل گذاری و یا گشودن قفل کنترل کرده اند.

در منبع [۱۹] در طرحی برای احراز هویت برای اختفا بیشتر از تگ موقعیت استفاده کرده اند. توابع دیگری که در این طرح استفاده شده است عبارتند از :تابع هش یکطرفه و عملیات باینری.

در منبع [۲۰] برای حفاظت سیستم در مقابل ردیابی از رهگیری رو به عقب استفاده کرده اند که در این طرح شناسه تگ هر زمان که گزارش داده می شد با استفاده از یک مکانیزم زنجیره ای Hash کم هزینه به روز رسانی میشد.

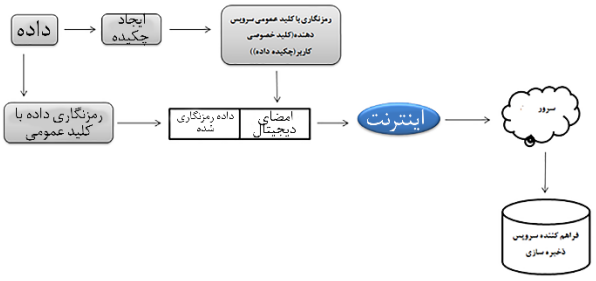
۳ – روش پیشنهادی

یکی از بخش های مهم روش پیشنهادی برای افزایش محرمانگی، استفاده از الگوریتم رمزنگاری مناسب است. در روش پیشنهادی، از الگوریتم RSA[7] که یک الگوریتم قوی در حفظ محرمانگی اطلاعات می باشد، استفاده شده است. یکی از معایب این الگوریتم نسبت به سایر الگوریتم های متقارن مانند AES[8] و DES[9] سرعت پایین آن است ولی در عمل امنیت بالاتری دارد. لذا در روش پیشنهادی رمزنگاری در سمت سرویس گیرنده(کاربر) انجام می گیرد. رمزنگاری و رمزگشایی در سمت سرویس گیرنده باعث می شود دیگر مشکل گلوگاه که از بزرگترین چالش های موجود در اینترنت اشیا است را نداشته باشیم همچنین بار کاری سرور کاهش می یابد.

(شکل-۱): رمزنگاری و ارسال به سرور

(Figure-1): Encrypt and send to server

در روش پیشنهادی دو سناریو ارائه می شود، یک سناریو برای ذخیره سازی امن اطلاعات بدون در نظر گرفتن قابلیت پردازش داده ها و سناریو دیگر با در نظر گرفتن قابلیت پردازش اطلاعات در سمت سرویس دهنده.



(شکل-۲): روش پیشنهادی

(Fiqure-2): suggested method

روش پیشنهادی برای ذخیره سازی امن اطلاعات در شکل (۲) آمده است. همانطور که در شکل (۲)

[7] Rivest–Shamir–Adleman

[8] Advanced Encryption Standard
[9] Data Encryption Standard

مشاهده می شود داده ها در سمت کاربر رمزنگاری شده و به همراه امضای دیجیتال به سرویس دهنده ارسال می شوند و سرویس دهنده داده های دریافتی را در سرورهای ذخیره سازی، بارگذاری می کند. در ادامه نحوه رمزنگاری داده ها و بارگذاری آن ها در سمت سرویس دهنده توضیح داده می شود.

رمزنگاری: یکی از بخش های مهم روش پیشنهادی برای افزایش محرمانگی استفاده از الگوریتم رمزنگاری مناسب است. در روش پیشنهادی از الگوریتم RSA که یک الگوریتم قوی در حفظ محرمانگی اطلاعات می باشد، استفاده شده است. در روش پیشنهادی رمزنگاری در سمت سرویس گیرنده(کاربر) انجام می‌گردد. رمزنگاری و رمزگشایی در سمت سرویس گیرنده باعث می شود دیگر مشکل گلوگاه که از بزرگترین چالش های موجود در اینترنت اشیا است را نداشته باشیم. همچنین بار کاری سرور کاهش می یابد.

نحوه رمزنگاری داده ها در سمت سرویس گیرنده: ابتدا در سمت سرویس گیرنده کاربر با استفاده از الگوریتم RSA کلید عمومی و خصوصی خودش را بدست می‌آورد. سپس کاربر با کلید عمومی اش داده ها را رمزنگاری کرده و به همراه امضای دیجیتال به سمت سرویس دهنده ارسال می کند

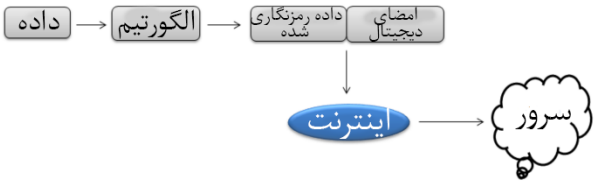
برقراری امنیت این داده ها در یک اجرا عملی نیست و امنیت نیز به درستی ایجاد نمی شود. بنابراین از طرح داده پردازی بصورت قطعه بلوک ها استفاده می‌شود که باعث ایجاد مفهوم رمزهای بلوکی می شود. متداول ترین مقدار بلوک، ۶۴، ۱۲۸، ۲۵۶ یا ۵۱۲ بیت است. می بینید که این مقادیر، توان دو هستند چرا که کامپیوترها داده ها را به صورت بایزی و با استفاده از محاسبات مدولی با ضریب دو پردازش می کنند. برای رمزگذاری بلوک های داده های بایزی نیاز به یک الگوریتم و یک کلید داریم تا طوری رمزگذاری کنیم که داده های رمزگذاری شده برای هکرها پیچیده و گیج کننده باشد. الگوریتم به صورت عمومی مطرح می شود اما کلید در اختیار کاربران غیر مجاز قرار داده نمی شود، بنابراین هکرها می توانند با تلاش برای شکستن پیام رمزگذاری شده بر قوت و توان رمز بیفزایند.

منطق رمز بلوکی به شرح زیر است :

- هر بیت از متن رمز باید وابسته به تمام بیت های کلید و تمام بیت های متن عادی باشد.
- نباید هیچ گونه مدرکی از رابطه آماری بین متن عادی و متن رمز وجود داشته باشد .

هدف الگوریتم رمزنگاری این است که طوری پیام را به هم ریزد که هیچ رابطه آشکاری بین متن رمز و متن عادی دیده نشود و این قاعده جایگزینی (s-boxes) و کلید حاصل می شود.

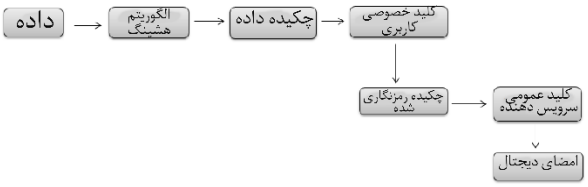
اگر تغییر یک بیت در متن عادی کمترین تاثیر را بر متن رمز داشته باشد، هکر می تواند با تغییر بیت ها به صورت معکوس از متن رمز به متن عادی برسد. بنابراین، کمترین تغییر در متن عادی به بیشترین تغییر در متن رمز انجامد که نتیجه آن انتشار و افشای متن است. جایگشت یا p-boxes عمل انتشار را انجام می دهد[۳].



(شکل - ۳): رمزنگاری و ارسال فایل به سرور

(Figure-3): Encrypt and send file to server

امضای دیجیتال: کاربر با الگوریتم ، چکیده پیام را به دست می آورد، سپس چکیده را با کلید خصوصی خود رمزنگاری کرده و سپس با استفاده از کلید عمومی سرویس دهنده(فرض میکنیم کاربر کلید عمومی سرویس دهنده را در اختیار دارد) مجددا رمزنگاری می کند. کاربر از امضای دیجیتال برای احراز هویت خودش در سمت سرویس دهنده استفاده می کند.



(شکل - ۴): نحوه ایجاد امضای دیجیتال

(Figure-4): How to create a digital signature

۴- ارزیابی

امنیت روش پیشنهادی:

ما برای ارزیابی روش پیشنهادی از چندین معیار استفاده کرده ایم همچنین برای مقایسه از روش ارائه شده در مقاله [۲۲ , ۲۳] استفاده کرده ایم نتایج مقایسه در ادامه توضیح داده شده اند.

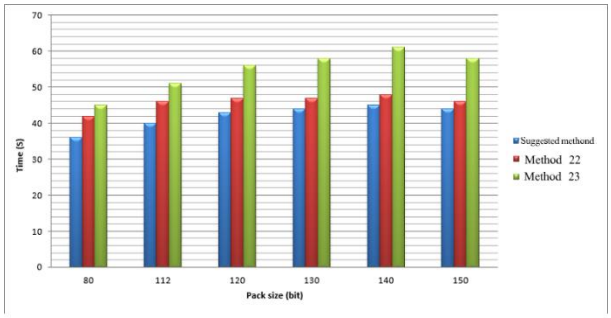
در مرجع [۲۲] رمزنگاری مبتنی بر ویژگی صورت گرفته است. در رمزنگاری مبتنی بر ویژگی کل اطلاعات رمز نمی شوند و فقط ویژگی که از اطلاعات استخراج شده است رمزنگاری می گردد. چون رمزنگاری سمت سرور صورت میگیرد، در حین انتقال اطلاعات در بستر شبکه از سیستم سرویس گیرنده به سرور ذخیره سازی امنیت اطلاعات به خطر می افتد و اخلال گران می توانند با استراق سمع به اطلاعات کاربر دسترسی پیدا کنند. در روش پیشنهادی این مشکل حل شده است، احراز هویت و رمزنگاری اطلاعات قبل از ارسال،هر دو با استفاده از رمزنگاری RSA که یک رمزنگاری با سطح امنیت بالا و روشی نامتقارن است صورت می گیرد. این روش در مقایسه با روش [۲۳] سطح امنیت بالاتری دارد، زیرا در مرجع نامبرده از RSA تنها برای تولید کلید استفاده شده و برای رمزنگاری الگوریتم Blowfish که جز الگوریتم های متقارن و حتی ضعیف تر از DES عمل می کند، استفاده شده است. پس روش پیشنهادی امنیت بالاتری نسبت به [۲۲] , [۲۳] دارد و امنیت اطلاعات در آن نسبت به مراجع نامبرده عملکرد بهتری دارد

بار کاری سرویس دهنده: در [۲۲] رمزنگاری سمت سرور انجام میگیرد که عملا بار کاری سرویس دهنده را افزایش می دهد، در صورتی که در روش پیشنهادی سرورهای ذخیره سازی تنها وظیفه ذخیره و بازیابی اطلاعات را بر عهده دارند و درگیر مسائل دیگری مانند رمزنگاری و مدیریت حساب کاربری نمی شوند، پس بار کاری سرور کاهش می یابد و مشکل گلوگاه نیز بر طرف خواهد شد.

جایگذاری فایل: در [۲۲] , [۲۳] اطلاعات بصورت یکپارچه روی یک رسانه ذخیره سازی، ذخیره می‌شوند که در صورت مورد حمله قرار گرفتن سرور،

کل اطلاعات فاش خواهند شد. در صورتی که در روش پیشنهادی اطلاعات به بخش های کوچکتری شکسته شده و روی چندین رسانه توزیع می شوند. بدین شکل ریسک از بین رفتن اطلاعات کاهش می یابد و با مورد حمله قرار گرفتن یک سرور، کل اطلاعات فاش نخواهد شد. همچنین برای واکشی اطلاعات نیز چون اطلاعات همزمان از چندین سرور واکشی می شوند سرعت نیز بالا می رود.

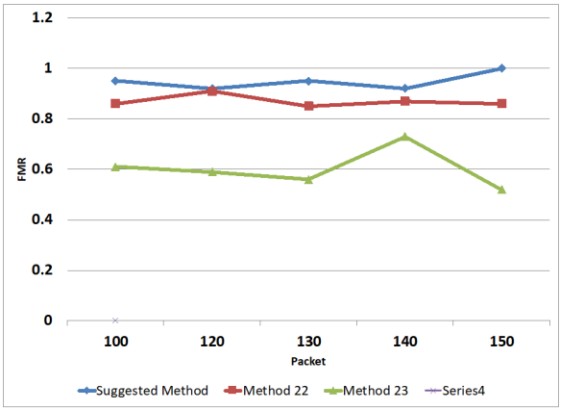
معیار زمان اجرا: در این معیار مدت زمانی که طول کشیده است تا درخواستهای احرازهویت به طور کامل انجام شود مورد مقایسه قرار گرفته است، در هر مرحله اندازه بسته ها بیشتر شده است که در شکل ۵ قابل مشاهده میباشد.



(شکل – ۵):زمان اجرا

(Fiure-5):Run Time

معیار FMR: نرخ تطابق جعلی یا FMR برابر است با احتمال قبول یک نمونه نادرست به‌عنوان نمونه‌ای اصلی. از این معیار به نسبت قبول نادرست یا FAR نیز یاد می‌شود. به بیان ساده‌تر این معیار یعنی احتمال اینکه اثر فرد B به‌اشتباه به‌عنوان اثر فرد A شناخته شده باشد . در شکل ۶ معیار FMR برای روش پیشنهادی و روش های [۲۲] و[۲۳] به ازای بسته های مختلف مورد ارزیابی قرار گرفته است.

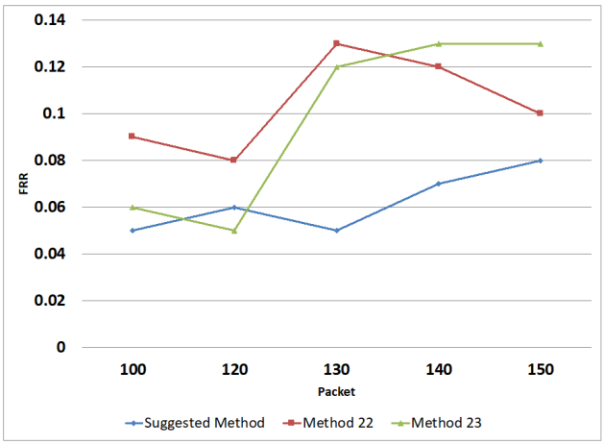


(شکل – ۶):مقایسه معیار FMR

(Fiqure-6): Comparison of FMR criteria

معیار عدم پذیرش اشتباه : این خطا زمانی رخ می دهد که یک سیستم بیومتریک کاربر دارای مجوز را به اشتباه نپذیرد. یا FRR به False Reject Rate

معنی نرخ عدم پذیرش اشتباه که خطای شماره یک هم نامیده می شود و درصد دفعاتی که عدم پذیرش اشتباه رخ مید هد را نشان می دهد



(شکل – ۷):مقایسه معیار FRR

(Figure-7): Comparison of FRR criteria

۵ – نتیجه گیری

در این مقاله توانستیم یک روشی جهت احراز هویت و همچنین جهت ذخیره و بازیابی اطلاعات

کاربران در اینترنت اشیا ارائه دهیم. با استفاده از روش پیشنهادی کاربران می توانند اطلاعات خود را با امنیت خاطر بیشتر نسبت به روش های مشابه و بدون اطلاع از نحوه و مکان ذخیره سازی، داده هایشان را به سرورهای ذخیره سازی اینترنت اشیا بسپارند. هچنین با رمزنگاری و امضای دیجیتال جهت احراز هویت علاوه بر دستیابی به امنیت سطح بالا، مشکل گلوگاه که اغلب روش های ذخیره سازی با آن روبرو هستند حل شود. همچنین در این مقاله دو سناریو طراحی شد یک سناریو برای زمانی که هدف ذخیره سازی داده ها است و سناریوی دیگر برای زمانی که هدف پردازشش داده ها است. در مبحث سناریو ذخیره سازی داده ها از الگوریتم رمزنگاری RSA استفاده شد، علی رغم اینکه ممکن است توان پردازشی و تاخیر بالایی به سیستم بدهیم بنابراین پیشنهاد می‌شود برای متونی که از نظر امنیتی نیاز به امنیت بالایی دارند استفاده از الگوریتم RSA که در سناریو اول طرح شده است، ایده مناسبی باشد. همچنین برای متون بزرگ پیشنهاد نمیکنیم از ایده طرح شده در سناریو اول استفاده شود چون زمانبر بوده و تاخیر کار بالایی دارد. در سناریو دوم نیز در مواردی که به نظر می رسد خیلی سرعت مدنظر نظر نباشد و بخواهیم امنیت را هم در پردازش مدنظر قرار بدهیم. استفاده از الگوریتم رمزنگاری AES به دلیل سرعت بالا و سبک بودن، گزینه مناسبی باشد، این در حالی است که شاید برای پردازش بحث امنیت خیلی مورد توجه قرار نگرفته شده باشد.

۶ – مراجع

1. T.Dimitriou.A lightweight RFID protocol to protect against traceability and cloning attacks. In Conference on Security and Privacy for Emerging Areas in Communication Networks | SecureComm 2005, pages 5966, Athens, Greece, September 2005. IEEE.
2. Alizadeh M., Zamani M., Shahemabadi A. R., Shayan J. & Azanik A., A Survey on Attacks in RFID Networks, Open International Journal of Informatics, 1(1), 2013.
3. Mitrokotsa A., Rieback M. R. & Tanenbaum A. S., Classifying RFID Attacks and Defenses. Information Systems Frontiers, 12(5), 2010
4. Khedr W. I., SRFID: A Hash-based security scheme for low cost RFID systems, Egyptian Informatics Journal, 14(1), 2013.
5. Cho J. S., Yeo S. S. & Kim S. K., Securing against brute-force attack: A Hash-based RFID mutual authentication protocol using a secret value, Computer Communications, 34(3), 2011.
6. C.Lim and T.Kwon.Strong and robust RFID authentication enabling perfect ownership transfer. In P.Ning, S.Qing, and N.Li, editors, Conference on Information and Communications Security | ICICS '06, volume 4307 of Lecture Notes in Computer Science, pages 1-20, Raleigh, North Carolina, USA, December 2006. Springer-Verlag.
7. B.Song.Server Impersonation Attacks on RFID Protocols. In Second Inter-national Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies | UBICOMM 08, pages 50-55, Valencia, Spain, October 2008. IEEE Computer Society.
8. 47. Ye, N.; Zhu, Y.; Wang, R.C.; Malekian, R.; Min, L.Q. An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things. Int. J. Appl. Math. Inf. Sci. 2014, 8, 1617–1624.
9. Mahalle, P.N.; Prasad, N.R.; Prasad, R. Object Classification based Context Management for Identity Management in

Internet of Things. Int. J. Comput. Appl. 2013, 63, 1–6
10. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, pp. 2266-2279, 2013.
11. E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," in International Workshop on Secure Interner of Things(SIOT) 2015.
12. P. Gope and T. Hwang, "A Realistic Lightweight Authentication Protocol Preserving Strong Anonymity for Securing RFID System," Computers & Security, vol. 55, pp. 271–280, 2015.
13. P. Gope and T. Hwang, "Enhanced Secure Mutual Authentication and Key Agreement Scheme Preserving User Anonymity in Global Mobile Networks," Wireless Personal Communications, vol. 82, pp. 2231-2245, 2015.
14. T. Hwang and P. Gope, "Provably secure mutual authentication and key agreement scheme with user anonymity," in Information, Communications and Signal Processing (ICICS) 2013 9th International Conference on, 2013, pp. 1-5.
15. P. Gope and T. Hwang, "Untraceable sensor movement in distributed IoT infrastructure," Sensors Journal, IEEE, vol. 15, pp. 5340-5348, 2015
16. P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," International Journal of Distributed Sensor Networks, vol. 2014, 2014.
17. M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," Systems Journal, IEEE, vol. 8, pp. 749-758, 2014.
18. P. N. Mahalle, N. R. Prasad, and R. Prasad, "Threshold Cryptographybased Group Authentication (TCGA) scheme for the Internet of Things (IoT)," in Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014 4th International Conference on, 2014, pp. 1-5.
19. P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in Wireless Communications and Networking Conference (WCNC), 2014 IEEE, 2014, pp. 2728-2733.
20. P. Gope and T. Hwang, "Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme With User Anonymity for Secure Communication in Global Mobility Networks," Systems Journal, IEEE, vol. PP, pp. 1 - 10, 2015.
21. Asadpour, Farshad, and Shamsollah Ghanbari. "Presenting a New Method of Authentication for the Internet of Things Based on RFID." International Conference on Soft Computing and Data Mining. Springer, Cham, 2018.