Vol. 6, No. 18, Apr-Jun 2026 (75-94)

Journal of New Achievements in Electrical, Computer and Technology (JNAECT)

مجله دستاوردهای نوین در برق،کامپیوتر و فناوری

دوره ۶، شماره ۱۸، بهار ۱۴۰۵ (۹۴-۷۵)

journal homepage: https://jnaect.ir

تامین امنیت شبکه های کامپیوتری رایانش ابری با استفاده از الگوریتم پویای رمزنگاری FR ۱

محمد هادی نیا

Mohammad.hadinia1@gmail.com

فوق لیسانس مهندسی فناوری اطلاعات گرایش امنیت، اطلاعاتدانشگاه بین المللی امام رضا (علیه السلام)

چکیده

رمزنگاری دانشی است که به بررسی و شناخت اصول و روش های انتقال یا ذخیره اطلاعات به صورت امن، حتی اگر مسیر انتقال اطلاعات و کانال های ارتباطی یا محل ذخیره اطلاعات ناامن باشند می پردازد. رایانش ابری یکی از فرصت های تکنولوژیک نوظهور است که توانسته به مقدار قابل توجهی نیاز به خرید سخت افزارهای تخصصی و در نتیجه هزینه های مربوط به آن را برای کاربران کاهش دهد. یکی از بخش های مهم رایانش ابری، فضای ذخیره ابری است. کاهش چشمگیر هزینه ها و سرعت پردازش بالا در فضای ذخیره ابری موجب شده است که پایگاه داده های ابری با اقبال زیادی در میان کسب و کارهای مختلف روبرو شود. اما از سوی دیگر پایگاه داده های ابری با چالش های امنیتی جدی مواجه هستند. همین موضوع مبین اهمیت تلاش برای ارتقاء امنیت پایگاه داده های ابری است. یکی از روشهای مقبول در این زمینه،روش رمزنگاری است. در این مقاله به بررسی امنیت مجازی سازی رایانش ابری با استفاده از کلید های متقارن و نامتقارن قرار خواهد گرفت و در نتیجه الگوریتمی پویا به نام FR1 طراحی و شبیه سازی شده که امنیت را چند برابر بالاتر برده و باعث ایجاد عدم هک اطلاعات رمز گذاری شده خواهد شد.

واژه‌های کلیدی: رمزنگاری و رمزگشایی ، شبکه های کامپیوتری، رایانش ابری

.

مقدمه

سیستم های محاسباتی بطور گسترده ای در حال کامل شدن هستند تا بتوانند پاسخگوی نیازهای بشر در مسائل و کاربردهای مختلف علمی، تجاری، اجتماعی و ... باشند. این تکامل در ابعاد مختلفی صورت گرفته است. قدرت و توان محاسباتی و پردازش اطلاعات، ظرفیت ذخیره سازی اطلاعات، در دسترس پذیری بیشتر منابع و ... از ابعاد مختلف تکامل سیستم های محاسباتی محسوب می شود. رایانش ابری یکی از رویکرد های جدید محاسباتی است که در چند سال اخیر مورد توجه بسیار قرار گرفته است و بطور فزاینده ای در حال گسترش است. تعاریف زیادی از مجازی سازی وجود دارد. در یک تعریف کلی، مجازی سازی به معنای ایجاد یک سطح انتزاعی از منابع محاسباتی است که در سطوح مختلف یک رایانه قابل اعمال است. سطوح سخت افزار، برنامه کاربردی و سیستم عامل برخی از مواردی هستند که ایجاد انتزاع می تواند در آنها انجام شود، امروزه محاسبات با توسعه رایانش ابری و خدماتی که مزایای متعددی مانند انعطاف پذیری، مقیاس پذیری و سودآوری را ارائه می دهد، وارد مرحله جدیدی شده است. یکی از مهمترین ویژگیهایی که رایانش ابری باید داشته باشد، انعطاف پذیری است. به طوری که انعطاف پذیری زیرساختهای ابری و مزایای اقتصادی به انگیزههای بزرگ در ادامه پذیرش ابر تبدیل شده است. اما استفاده از ابرها، به خصوص ابرهای عمومی، موضوع امنیت را پررنگ تر می کند. به طوری که طیف وسیعی از کاربردهای رایانش ابری توجه آکادمیک را به امنیت در هنگام ذخیره سازی، مدیریت و پردازش دادهها جلب کرده است. لذا ارائه راهکارهای امنیتی در ابرهای عمومی بسیار مهم است(فاطمه رمضانی و علیرضا چمکوری،۱۴۰۴). رایانش ابری اخیرا۱ به عنوان یک الگو برای میزبانی و تحویل سرویس ها بر روی اینترنت پدیدار گشته است . به عبارت دیگر رایانش ابری مجموعه ای از منابع مجازی و مقیاسپذیر است که قابلیت ارائه خدمات مورد نیاز کاربران با پرداخت بر اساس میزان استفاده آنها از سرویس ها می باشد. امنیت و حفظ حریم خصوصی بزرگترین مانع بر سر راه پذیرفته شدن این سبک محاسباتی بطور گسترده می باشد. با این وجود بعضی از نیازهای امنیتی و حفظ حریم خصوصی در برنامه های ابری به مدل سرویس یا استقرار ابری مورد استفاده بستگی دارد، اما با اجرای دقیق یک مدل مبتنی بر ابر، می توان بالاترین سطوح امنیت فیزیکی ، شبکه ای، برنامه های کاربردی، دادهها و سیستم های داخلی را تضمین کرد. موارد مهمی همچون رمزنگاری اطلاعات و احراز هویت کاربران نیز به طور مرتب در حال اجراست(فرزانه عماد،۱۴۰۳). طرح خوشه بندی در شبکه های حسگر بیسیم استفاده موثر از منابع انرژی را برای گره های حسگر فراهم می کند و بطور موثر طول عمر این شبکه ها را افزایش می دهد. از آنجایی که شبکه های حسگر بیسیم کاربردهای مهم و بسیار زیادی دارند، حملات به این شبکه ها در حالت وسعه است. اگرچه مطالعات زیادی برای امنیت خوشه بندی در شبکه های حسگر بیسیم انجام شده است، ولی بدلیل توسعه روزافزون این شبکه ها، مسیله امنیت بیشتر از قبل باید مورد توجه قرار بگیرد. رمزنگاری منحنی بیضوی با توجه به کارایی بالا، هزینه محاسباتی کم و ا ندازه کوچک کلید، اخیرا مورد توجه محققان زیادی قرار گرفته است و می تواند در امنیت خوشه بندی شبکه های حسگر بیسیم بسیار موثر باشد(داود نوری و همکاران، ۱۳۹۲). سیستم بازیابی اطلاعات خصوصی سیستمی است که به کلاینت اجازه می دهد که یک داده را درخواست کند بدون اینکه سرور یا هر شخص دیگری از محل آن داده درخواستی اطلاع پیدا کند. در اکثر این سیستم ها از روش های رمزنگاری برای تولید پرس و جوهای رمزنگاری شده استفاده می شود تا مکان داده های درخواستی در ا ختیار افراد قرار نگیرد. رمزنگاری منحنی بیضوی جزو روش های رمزنگاری کلید نامتقارن است که در آن داده ها بر اساس نقاطی بر روی منحنی نگاشت می شوند و با توجه به خواص جالب جمع نقاط در این روش، امکان رمزنگاری داده ها مهیا می شود. همچنین بر اساس اصل لگاریتم گسسته منحنی بیضوی امکان رمزگشایی داد در حد مطلوبی کاهش می یابد(ایران حکمتیان،۱۳۹۶). لذا در این مطالعه به بررسی تامین امنیت شبکه های کامپیوتری رایانش ابری با استفاده از الگوریتم پویای رمزنگاری FR ۱ پرداخته شد.

پیشینه تحقیق

سیدمهدی سیادتیان و احمد فراهی در سال ۱۴۰۰ به مطالعه ای تحت عنوان مروری بر روشهای رمزنگاری پایگاه داده های ابری پرداختند در این تحقیق تلاش شده است با شناسایی روش های معمول رمزنگاری در حیطه پایگاه داده های ابری، ضمن استخراج مزایا و معایب هر یک از این روش ها، عوامل موثر در انتخاب یک روش رمزنگاری متناسب با نوع پایگاه داده ابری تبیین شوند. به این ترتیب نتایج این تحقیق هم می تواند به محققان این حوزه در فرآیند مطالعاتی کمک رساند و هم می تواند توسط افراد علاقمند به اجرای روش های رمزنگاری در پایگاه داده های ابری به کار رود(سیدمهدی سیادتیان و احمد فراهی،۱۴۰۰).

فاطمه رمضانی و علیرضا چمکوری در سال ۱۴۰۴ به مطالعه ای تحت عنوان بهبود امنیت داده در رایانش ابری عمومی با استفاده از یک معماری ترکیبی مبتنی ECC, AES پرداختند هدف از این پژوهش نیز ارائه روش کارآمد برای حفظ حریم خصوصی و امنیت دادهها در یک ابر عمومی با استفاده از ترکیب الگوریتمهای رمزنگاری است. از اینرو الگوریتمی ترکیبی با نام ECC - AES ارائه و در نرم افزار متلب پیاده سازی و مورد آزمایش قرار گرفت. دادههای مورد آزمایش شامل مجموعه دادههای تصویری، ۳۲۳، ۴۸۳ و ۶۳۰ بود و به منظور ارزیابی قدرت الگوریتم طول کلیدها نیز ۶۴، ۱۲۸، ۱۹۲ و ۲۵۶ انتخاب و الگوریتم ارائه شده با سایر الگوریتمها شامل Blowfish، AES و DES مقایسه شده است. نتایج به دست آمده نشان داد که الگوریتم ارائه شده در مقایسه با الگوریتمهای گذشته، سرعت بسیار بالا در رمزگذاری و رمزنگاری دارد(فاطمه رمضانی و علیرضا چمکوری،۱۴۰۴).

ایمان سلطانی و شیوا مختاری در سال ۱۳۹۸ به مطالعه ای الگوریتم رمزنگاری AES پرداختند در این مقاله ابتدا توضیح مختصری از روش رمزنگاری متقارن ونامتقارن گفته شده و کلیدهای رمزنگاری مورد بحث قرار گرفته و در ادامه الگوریتم رمزنگاری Rijndael که در حال حاضر بعنوان استاندارد رمزگاری پیشرفته یا به عبارت دیگر Advanced Encryption Standard)AES) شناخته می شود بررسی خواهد شد. در انتها نیز نقاط قوت ASE وتفاوت آن با رمزنگاری های دیگر و حملات صورت گرفته بر روی آن، مورد بحث قرار می گیرد(ایمان سلطانی و شیوا مختاری،۱۳۹۸).

جواد حمیدزاده و همکاران در سال ۱۳۹۴ به مطالعه ای تحت عنوان استفاده از منطق فازی در فرآیند رمزنگاری و رمزگشایی اطلاعات بر روی GPU پرداختند در این مقاله هدف به دست آوردن این حد آستانه با استفاده از منطق فازی در سیستم های مختلف می باشد. این سیستم فازی با در نظر گرفتن سه عامل کلیدی قدرت GPU نسبت به CPU، سرعت انقال اطلاعات به حافظه ی GPU و زمان انجام آماده سازی های اولیه برای انجام عملیات، حد آستانه مناسب را تخمین می زند.آزمایش ها نشان می دهد که انجام عملیات رمزنگاری به این روش بر روی GPU می تواند باعث افزایش کارایی اجرا تا هشت برابر نسبت به CPU شود(جواد حمیدزاده و همکاران،۱۳۹۴).

میثم بهروزیان در سال ۱۴۰۴ به مطالعه ای تحت عنوان چارچوب ترکیبی یادگیری فدرال و رمزنگاری منحنی بیضوی برای تشخیص ناهنجاری در شبکه های اینترنت اشیاء با تضمین حریم خصوصی و کارایی بهینه پرداخت در این مقاله، یک چارچوب ترکیبی مبتنی بر یادگیری فدرال (Federated Learning) و رمزنگاری مبتنی بر منحنی بیضوی (ECC) برای تشخیص ناهنجاری در شبکه های IoT ارائه می شود. در روش پیشنهادی، هر گره IoT با استفاده از یک شبکه عصبی پیچشی (CNN) به صورت محلی آموزش می بیند و گرادیان های محاسبه شده با استفاده از الگوریتم ECC رمزنگاری شده و به سرور مرکزی ارسال می شوند. سرور مرکزی بدون دسترسی به داده های خام، به کمک عملگرهای هومومورفیک مبتنی بر

منحنی بیضوی، گرادیان های دریافتی را تجمیع و مدل جهانی را به روزرسانی می کند. برای اعتبارسنجی روش، از دو دیتاست عمومی TON_IoT و BoT-IoT استفاده شده است. نتایج شبیه سازی (روی ماشین محلی با پردازنده Intel i H۷-۹۷۵۰ و ۱۶ گیگابایت رم) نشان می دهد که روش پیشنهادی به دقت متوسط ۹۲.۳٪ و مقدار Score۱F- برابر با ۰.۹۱ دست می یابد، در حالی که سربار زمانی رمزنگاری تنها ۱۲٪ افزایش می یابد. این ارقام نسبت به روش های متمرکز مرسوم، بهبود قابل ملاحظه ای در حفظ حریم خصوصی بدون کاهش دقت ایجاد می کنند(میثم بهروزیان،۱۴۰۴).

رضا شاعری نیا و همکاران در سال ۱۴۰۴ به مطالعه ای تحت عنوان ارائه یک طرح احراز هویت و توافق کلید ایمن و کارا مبتنی بر رمزنگاری منحنی بیضوی برای محیط های اینترنت اشیاء صنعتی پرداختند در این پژوهش، یک طرح تبادل کلید احراز هویت مبتنی بر رمزنگاری منحنی بیضوی (ECC) برای ارتباط امن بین دستگاه ها ارائه شده است. پروتکل پیشنهادی در چهار مرحله شامل راه اندازی، ثبت نام، احراز هویت و توافق کلید، و به روزرسانی کلید های خصوصی/عمومی انجام می پذیرد. تحلیل امنیتی نشان می دهد که طرح پیشنهادی در مقایسه با روش های موجود، ایمنی باالتری در برابر حمله های شخص میانی، جعل، نشت پارامتر مخفی و تسخیر کلید دارد. همچنین، بهینه سازی محاسباتی و کاهش تعداد عملیات رمزنگاری، آن را برای محیط های صنعتی با منابع محدود مناسب می سازد. این پژوهش گامی مهم در جهت تضمین اعتمادپذیری و امنیت دستگاه های IIoT است و راه را برای پیاده سازی سیستم های صنعتی مقاوم در برابر تهدیدات امنیتی هموار می کند(رضا شاعری نیا و همکاران،۱۴۰۴).

رضا شفارودی در سال ۱۴۰۳ به مطالعه ای تحت عنوان ساختارهای جبری در رمزنگاری پست کوانتومی پرداخت این پژوهش به بررسی جامع ساختارهای جبری که پایه و اساس رمزنگاری پست کوانتومی را تشکیل می دهند، می پردازد. مطالعه حاضر با تمرکز بر چهار خانواده اصلی رمزنگاری پست کوانتومی شامل رمزنگاری مبتنی بر شبکه، رمزنگاری مبتنی بر کد، رمزنگاری مبتنی بر چندجمله ای های چندمتغیره و رمزنگاری مبتنی بر ایزوژنی، ساختارهای جبری زیربنایی این سیستم ها را مورد تحلیل قرار می دهد. با استفاده از روش تحلیل محتوای کیفی و مرور نظام مند ادبیات موجود، این پژوهش چالش های ریاضی و الگوهای جبری را در طراحی و تحلیل امنیت الگوریتم های پست کوانتومی بررسی می کند. یافته های این مطالعه نشان می دهد که ساختارهای جبری پیچیده مانند شبکه های سخت، کدهای تصحیح خطا، چندجمله ای های چندمتغیره و گراف های ایزوژنی، نقش کلیدی در ایجاد الگوریتم های مقاوم در برابر حملات کوانتومی دارند. همچنین، چالش های موجود در استانداردسازی و پیاده سازی این الگوریتم ها مورد بحث قرار گرفته و مسیرهای آتی تحقیقات در این حوزه پیشنهاد شده است(رضا شفارودی،۱۴۰۴).

محمدعلی شریفی و همکاران در سال ۱۴۰۳ به مطالعه ای تحت عنوان بهبود الگوریتم های رمزنگاری با سیستم تراختنبرگ مطالعه ای درباره سرعت و امنیت پرداختند این تحقیق به بررسی کاربرد سیستم تراختنبرگ، یک روش برای محاسبات سریع ریاضی، در بهبود عملکرد الگوریتم های رمزنگاری، به ویژه در سیستم های رمزنگاری کلید عمومی مانند RSA و رمزنگاری منحنی بیضوی (ECC) می پردازد. فرآیندهای رمزنگاری به شدت به عملیات محاسباتی سنگینی مانند ضرب اعداد بزرگ، حساب مدولار و توان رسانی مدولار وابسته هستند. این مطالعه بررسی می کند که آیا روش های بهینه سازی شده ضرب و تقسیم در سیستم تراختنبرگ می توانند در این محاسبات رمزنگاری ادغام شوند تا زمان های رمزگذاری و رمزگشایی را کاهش دهند، بدون اینکه امنیت به خطر بیفتد. تحلیل دقیقی روی چگونگی بهینه سازی ضرب در طول توان رسانی مدولار و بهبود کارایی محاسبه معکوس های مدولار با استفاده از تکنیک های تراختنبرگ انجام شد. نتایج تجربی نشان می دهد که به کارگیری این روش ها منجر به کاهش قابل توجهی در زمان محاسبات کلیدی رمزنگاری، به ویژه در الگوریتم RSA، شده

است. ارزیابی های امنیتی نشان می دهد که با وجود بهبود در عملکرد، یکپارچگی ساختاری الگوریتم های رمزنگاری حفظ شده و هیچ گونه کاهش قابل ملاحظه ای در قدرت رمزنگاری مشاهده نمی شود(محمدعلی شریفی و همکاران،۱۴۰۳).

وهاب امبنی آذر و همکاران در سال ۱۴۰۲ به مطالعه ای تحت عنوان ارائه یک راهکار رمزنگاری سبک وزن به منظور تامین امنیت داده در اینترنت اشیا پرداختند در این مقاله یک راهکار رمزنگاری سبک وزن مبتنی بر رمزنگاری متقارن و نامتقارن جهت تامین امنیت داده در اینترنت اشیا ارائه شده است. در روش پیشنهادی در ابتدا داده اصلی توسط الگوریتم متقارن بلوفیش رمزنگاری می شود و سپس کلید آن¬ به کمک الگوریتم رمزنگاری خم¬های بیضوی ایمن¬سازی می شود تا در نتیجه بتوان در زمان کم و با امنیت بالا امنیت داده را در زیرساخت¬های مبتنی بر اینترنت اشیا تامین کرد. در انتها راهکار پیشنهادی، از طریق شبیه ساز Eclipse و با آزمایش بر روی حجم داده ۲۰ تا ۱۰۰۰ کلیوبایت مورد ارزیابی قرار داده شده است. نتایج حاصل از شبیه¬سازی نشان می¬د¬هد که روش پیشنهادی در مقایسه با سایر الگوریتم¬های رمزنگاری از نظر معیارهای ارزیابی هم چون زمان اجرا و توان عملیانی رمزنگاری و رمزگشایی بهینه¬تر عمل می¬نماید. این نتایج؛ بیانگر آن است که راهکار پیشنهادی ضمن برقراری امنیت، کمترین تاثیر منفی را بر روی منابع پردازشی گره های IoT داشته است(وهاب امبنی آذر و همکارانف۱۴۰۲).

سجاد رضایی ادریانی و مهدیه سجادی در سال ۱۴۰۱ به مطالعه ای تحت عنوان رای گیری الکترونیکی بر اساس رمزنگاری همریخت در گروه خم بیضوی پرداختند در این مقاله، یک طرح انتخابات بر اساس رمزنگاری همریخت در گروه جمعی خم بیضوی بیان میشود که ویژگیهایی از جمله استحقاق، محرمانگی، بدون رسید بودن، عدم امکان اجبار و غیره را برآورده میسازد و بدلیل استفاده از گروه خم بیضوی، درکنار امنیت معادل، کارایی خوبی در مقایسه با طرحهایی که بر اساس مسئلهی تجزیه اعداد و مسئلهی لگاریتم گسسته هستند را ارائه میدهد(با کلید ۱۶۰بیتی خم بیضوی امنیت معادل کلید ۱۰۲۴ بیتی RSA دارد). هر چند انتخابات مبتنی بر رمزنگاری همریخت و مسالهی لگاریتم گسسته در طرح هوزتی آمده است ولی روش مستحکمتر ارائه شده با تغییرات لازم و همچنین با ارائهی یک امضای کور که متناسب با طرح رای گیری، سعی شده است که این روش نسبت به مباحث ارائه شده تا به امروز امنتر باشد(سجاد رضایی ادریانی و مهدیه سجادی،۱۴۰۱).

نرگس اسدنجفی و مهدی ملا مطلبی در سال ۱۳۹۹ به مطالعه ای تحت عنوان بهبود احراز هویت در خانه هوشمند مبتنی بر رمز یکبار مصرف و رمزنگاری منحنی بیضوی پرداختند در این مقاله، روشی برای بهبود احراز هویت افراد، مبتنی بر رمز یکبار مصرف با استفاده از کارت هوشمند و الگوریتم رمزنگاری منحنی بیضوی در سامانه خانه هوشمند، ارائه‌شده است. ارزیابی روش پیشنهادی توسط منطق بن و در محیط نرم-افزار آویسپا انجام شده است. نتایج ارزیابی-ها حاکی از بهبود احراز هویت متقابل بین کاربر و گره دروازه جهت مقابله با حملات متداول به خانه هوشمند، در مقایسه با روش‌های موجود است. به‌علاوه، روش پیشنهادی از حملات استراق سمع و حمله سرک-کشی جلوگیری می-نماید که اکثر روش‌های موجود، قادر به جلوگیری از آنها نیستند(نرگس اسدنجفی و مهدی ملا مطلبی،۱۳۹۹).

مریم عطایی نژاد و حمید براتی در سال ۱۳۹۸ به مطالعه ای تحت عنوان یک روش احرازهویت دوطرفه مبتنی بر رمزنگاری منحنی بیضوی در سیستم رادیوشناسه پرداختند در این مقاله یک پروتکل احرازهویت دوطرفه با استفاده از رمزنگاری منحنی بیضوی برای سیستمهای رادیو شناسه ارائه شده است که روشی کارآمد جهت شناسایی حملات مخرب میباشد. مزیت اصلی رمزنگاری منحنی بیضوی یک کلید با اندازه کوچکتر است؛ که این موضوع به معنی کاهش ذخیره سازی و انتقال مورد نیاز است، در نتیجه، یک سیستم منحنی بیضوی میتواند همان سطح از امنیت را که یک سیستم مبتنی بر RSA با ماژول های بزرگ و طول بلند کلید فراهم میکند را ایجاد کند، مزیت دیگر این نوع رمزنگاری عدم توانایی معکوس کردن فرآیندها می

باشد به این معنی که وقتی کلید عمومی را که از کلیدخصوصی شما ساخته شده است را اعلام میکنید، با معکوس کردن فرآیند کلید خصوصی شما قابل محاسبه نیست(مریم عطایی نژاد و حمید براتی،۱۳۹۸).

پرویز کشاورزی و محبوبه جعفری در سال ۱۳۹۷ به مطالعه ای تحت عنوان افزایش سرعت پیاده سازی سخت افزاری در رمزنگاری منحنی بیضوی در میدان محدود اول پرداختند در این مقاله برای کاهش پیچیدگی محاسبات و هم چنین افزایش سرعت سیستم رمزنگاری منحنی بیضوی در میدان محدود اول، از روشی استفاده شده است که باعث افزایش سرعت در محاسبات و در نتیجه سرعت سیستم می گردد. در این روش پیشنهادی برای انجام عملیات معکوس پیمانه۱ که عملیات وقتگیر و پیچیده ای می باشد از روشی استفاده کردیم که بجای استفاده از الگوریتم های پیچیده، با استفاده از یک روش ساده و یک جدول پیشنهادی محاسبات معکوس پیمانه در یک کلاک پالس انجام می شود که باعث افزایش سرعت سیستم رمزنگاری منحنی بیضوی می گردد(پرویز کشاورزی و محبوبه جعفری،۱۳۹۷).

ایران حکمتیان در سال ۱۳۹۶ به مطالعه ای تحت عنوان طراحی یک سیستم بازیابی اطلاعات محرمانه مبتیی بر رمزنگاری می‌حنی بیضوی پرداخت در این مقاله یک سیستم بازیابی اطلاعات خصوصی مبتنی بر روش رمزنگاری منحنی بیضوی ارایه می شود که علاوه بر داشتن امنیت در سطح قابل قبول به دلیل برخی ویژگی های این روش از جمله طول کوتاه کلیدها و داده های رمزنگاری شده، میزان هزینه ارتباطی را در محیط های توزیع شده تا سطح قابل توجهی کاهش می دهد(ایران حکمتیان،۱۳۹۶).

حسین نیک خواه در سال ۱۳۹۷ به مطالعه ای تت عنوان افزایش امنیت و کاهش مصرف انرژی در شبکه حسگر بی سیم با استفاده از رمزنگاری منحنی بیضوی پرداخت این مقاله یک راه حل عملی برای احراز هویت همه پخشی چند کاربر و مبتنی بر رستگاری منحنی ایزدی در شبکه های حسگر رییس این پیشنهاد شده است. در مقایسه با کارهای مشابه و از جمله روش فن و همکارانش که جدیدترین آن ها است ، پیچیدگی زمانی مورد نیاز روش پیشنهادی در این مقاله به طور چشمگیری کاهش یافته است. علاوه بر این امنیت قابل اثبات را فراهم کرده و پیاده سازی ساده ای دارد. بنابراین روش پیشنهادی مناسب برای به کارگیری در شبکه های حسگر بایستی می باشد. روش پیشنهادی با تاکید بر ماهیت تولید و تایید امضای دیجیتال در بخش های جداگانه، باعث کاهش هزینه محاسبات می شود. انتهای این مقاله برای اثبات درستی عملکرد روش پیشنهادی با استفاده از زبان برنامه نویسی سی شارپ ، عملیات شبیه سازی روش پیشنهادی صورت گرفته و نتایج این شبیه ساز در قسمت نتیجه گیری مورد تحلیل و بررسی قرار خواهند گرفت(حسین نیک خواه،۱۳۹۷).

سارا همتی و شیوا تقی پورعیوضی در سال ۱۳۹۵ به مطالعه ای تحت عنوان بررسی انواع روش و الگوریتم های رمزنگاری پرداخت این مقاله انواع الگوریتم رمزنگاری مورد بررسی قرار گرفته است. طبقه بندی توابع و الگوریتم-های مورد استفاده در رمزنگاری بر اساس تعداد کلید به دو دسته کلی الگوریتم های رمزنگاری متقارن و نامتقارن تقسیم می شوند. نکته اساسی در طراحی الگوریتم های رمزنگاری انتخاب کلید مناسب می باشد. در هنگام استفاده از الگوریتم های رمزنگاری بایستی در نظر داشت که سری ماندن پیام صرفاً به مخفی و محرمانه بودن کلید رمز وابسته است. بنابراین انتخاب کلید رمز در کنار الگوریتم مناسب بسیار ضروری می باشد. هدف این پژوهش انتخاب معیارهای مهم به منظور ایجاد یک سیستم امن می باشد. در این مقاله مزایا و معایب الگوریتم های مختلف رمزنگاری و روش پیاده سازی آنها بررسی می شود.معیارهای مهم به منظور انتخاب یک الگوریتم مناسب شامل زمان اجرای الگوریتم، پیچیدگی الگوریتم، مصرف انرژی کمتر، میزان امنیت الگوریتم و بهره وری می باشند(سارا همتی و شیوا تقی پورعیوضی،۱۳۹۵).

مبانی نظری

رایانش ابری :(cloud computing) برای شناخت بهتر رایانش ابری از دید زیرساخت، ابتدا نگاهی به سیر تکاملی سیستم های محاسباتی از ابتدا تا کنون می اندازیم تا بتوانیم جایگاه آن را در بین دیگر سیستم ها تشخیص دهیم. اگر mainframe ها را بعنوان نسل اول سیستم های محاسباتی در نظر بگیریم ، ما با یک سیستم بسیار بزرگ مواجه بودیم که کاربران از طریق یک ترمینال واحد به آن دسترسی پیدا می کردند. به مرور این سیستم ها کوچکتر شدند و با توان پردازشی بیشتر و قیمت کمتر، بصورت رایانه های شخصی در اختیار همه کاربران قرار گرفتند. سپس این امکان فراهم شد که با اتصال مجموعه ای از این سیستم های کوچک، شبکه ای با توان پردازشی بیشتر فراهم نمود تا پاسخگوی نیازهای پردازشی بیشتر و سنگین تر باشند. اما نیازهای پردازشی به شکل فزاینده ای در حال افزایش بودند و نیاز به سیستم های محاسباتی بزرگتر و قوی تر احساس شد . بنابراین تعداد زیادی از این شبکه ها بصورت اختصاصی در سرتاسر اینترنت به هم متصل شدند و شبکه محاسبات توری را بوجود آوردند. در این بین مشاهده شد که میلیون ها کاربر در اینترنت وجود دارند که در اکثر اوقات از تمام توان رایانه خود استفاده نمی کنند و سیستم محاسباتی دیگری شکل گرفت تا کاربرانی که تمایل داشته باشند، زمان های بیکار سیستم خود را برای کارهای محاسباتی عام المنفعه هدیه کنند. بنابراین تعداد بسیار زیادی منبع محاسباتی کوچک در شبکه ای تحت عنوان محاسبات داوطلبانه به هم پیوستند و توان پردازشی عظیمی را بوجود آوردند. اما هنوز منابع بسیار زیاد دیگری در سازمان ها و مراکز داده اینترنتی وجود داشت که تمام ظرفیت آنها بطور کامل بکارگرفته نشده بود. این منابع نمی توانستند در شبکه محاسبات توری بصورت اختصاصی بکارگرفته شوند، زیرا برای آنها وظیفه دیگری تعریف شده بود. در عین حال امکان استفاده از آنها در شبکه داوطلبانه هم وجود نداشت، چون فلسفه وجودی آنها، کاربردهای تجارت بود. به این ترتیب رویکرد جدیدی شکل گرفت که بتوان با استفاده از فناوری های مجازی سازی این منابع را بصورت قابل انعطاف و پویا برای کاربردهای مختلف مورد استفاده قرار داد و از تمام ظرفیت آن ها بطور موثر استفاده کرد. این فناوری رایانش ابری در لایه زیرساخت نام داشت که امکان استفاده از منابع محاسبات و ذخیره سازی را بصورت یک سرویس بر حسب نوع نیاز فراهم می آورد. در حقیقت با ایجاد یک لایه انتزاعی بر روی کلیه منابع فیزیکی – خود (به کمک مجازی سازی) امکان مدیریت پویای منابع فیزیکی حاصل می شود .

رایانش ابری از کارآمدترین روش‌های هزینه برای استفاده، حفظ و ارتقای برنامه و داده است. نرم‌افزارهای مرسوم برای شرکت‌ها ، ادارات و ارگان های دولتی هزینه زیادی دارد، درحالی که رایانش ابری با هزینه‌های کمتری در دسترس است و سازمان‌ها می‌توانند هزینه‌های اجرایی سالانه خود را با استفاده از آن کاهش دهند. از دیگر مزایای استفاده از رایانش ابری، فضای تقریبا نامحدود برای ذخیره‌سازی است. از این رو دیگر نیازی نیست نگران کمبود فضای کافی یا افزایش فضای ذخیره باشید.

همچنین از آن‌جایی که همه اطلاعات شما در ابر ذخیره شده است، تهیه نسخه پشتیبانی (بک‌آپ گرفتن) از آن و بازگرداندن اطلاعات مشابه، بسیار ساده‌تر از ذخیره همان اطلاعات در یک وسیله فیزیکی است. بنابراین، بیشتر ارائه‌دهندگان خدمات ابری برای بازیابی اطلاعات رقابت می‌کنند.

سیر تکاملی محاسبات به گونه ای است که می توان آن را پس از آب، برق، گاز و تلفن به عنوان عنصر اساسی پنجم فرض نمود. در چنین حالتی، کاربران سعی می کنند بر اساس نیازهایشان و بدون توجه به اینکه یک سرویس در کجا قرار دارد و یا چگونه تحویل داده می شود، به آن دسترسی یابند. نمونه های متنوعی از سیستم های محاسباتی ارائه شده است که سعی

دارند چنین خدماتی را به کاربران ارئه دهند. برخی از این سیستم های محاسباتی عبارتند از: محاسبات کلاستری ، محاسبات توری و اخیراً محاسبات انبوه که از آن به عنوان رایانش ابری نیز یاد می شود.

دنیای محاسبات به سرعت به سمت توسعه نرم افزارهایی پیش می رود که به جای اجرا بر روی رایانه های منفرد، به عنوان یک سرویس در دسترس میلیون ها مصرف کننده قرار داده می شوند. از این نقطه نظر، محاسبات انبوه (رایانش ابری) از دید کاربران نهایی ساختاری شبیه به یک توده ابر دارد که به واسطه آن می توانند به برنامه های کاربردی از هرجایی از دنیا دسترسی داشته باشند. اما محاسبات انبوه از دید فرآهم کنندگان منابع زیرساخت، می تواند با کمک ماشین های مجازی شبکه شده ، به عنوان یک روش جدید برای ایجاد پویای نسل جدید مراکز داده، مورد استفاده قرارگیرد تا بتوانند یک زیرساخت قابل انعطاف برای ارائه انواع مختلف خدمات محاسباتی و ذخیره سازی در اختیار داشته باشند.

امنیت : (security) شیوه های مناسب امنیتی، در هر یک از جنبه های طراحی سیستم، پیاده سازی و استقرار آن وارد شده است. کاربردها باید بصورت امن و با واسط هایی که تنها داده های مناسب را برای کاربران مجاز ارائه می کنند ، طراحی شده باشند. در حین پیاده سازی، توسعه دهندگان باید مراقب کدهایی که منجر به آسیب پذیری ابر در مقابل تکنیک هایی نظیر buffer overflow یا Sql injection می شوند باشند. وقتی برنامه ارائه شد، سیستم های عامل باید امن شوند و هر سطح از نرم افزار با آخرین وصله های امنیتی، به روز نگه داشته شود . در رایانش ابری، برنامه ها در محیط های اشتراکی شبکه ارائه می شوند، و هر تکنیک ساده امنیتی، نظیر VLAN و Port filtering برای جداکردن و محافظت از انواع بخش های معماری برنامه کاربردی، نظیر جداکردن کاربران از همدیگر بکار برده می شود.

کلید متقارن و نامتقارن : (symmetric and asymmetric key) الگوریتم های رمزنگاری داده ها به طور کلی به دو دسته تقسیم می شوند.

الگوریتم های رمز متقارن: الگوریتم های کلاسیک در زمان خود به دلیل عدم وجود ابزارهای مدرن محاسباتی الگوریتم های خوبی به حساب می آمدند. رمزنگاری با این الگوریتم ها به طور عمده با استفاده از کاغذ و قلم صورت می گرفت که در دوره زمانی استفاده از انها , شکستن متون رمز شده, به آسانی امکان پذیر نبود. متون رمز شده بر اساس این دسته از الگوریتم ها با استفاده از ماشینهای محاسب به سادگی قابل تحلیل بوده و با استخراج الگوهای موجود در متون رمز شده, شکستن الگوریتم های مورد نظر به راحتی صورت می پذیرد.

مشکل دیگر الگوریتم های کلاسیک لو رفتن روش استفاده شده در الگوریتم بود به گونه ای که اگر فرد مهاجم اطلاعاتی در مورد الگوریتم رمزنگاری در اختیار داشت به سهولت میتوانست متن رمز شده را شکسته و به محتوی آن دسترسی پیدا می نمود.

در طراحی الگوریتم های رمزنگاری مدرن بجای مخفی نگاه داشتن الگوریتم رمزنگاری سعی می شود, کلید مورد استفاده در الگوریتم مخفی نگاه داشته شود. در هر بار اجرای فرایند رمزنگاری, الگوریتم ثابت مانده ولی کلید تغییر می کند. در این روش با آنکه عامل مهاجم در مورد الگوریتم رمزنگاری مطلع بوده ولی به دلیل عدم دسترسی به مقدار کلید مورد استفاده از در دسترسی به محتوی متن رمزنگاری شده عاجز خواهد بود.

الگوریتم های رمزنگاری مدرن به دو دسته متقارن و نامتقارن استفاده می شوند. الگوریتم های متقارن که بحث اصلی ما است, از نظر نحوه رمزنگاری دارای شباهت های بسیار زیادی با الگوریتم های کلاسیک می باشد. این الگوریتم ها از فرایند جا نشانی و جایگزینی استفاده نموده و علاوه بر این دو فرایند می توانند از فرایند XOR نیز استفاده کند.

از الگوریتم های متقارن برای رمز نگاری پیام استفاده می شود. امنیت پیام در الگوریتم های رمزنگاری متقارن به مخفی نگاه داشتن کلید و طول کلید مورد استفاده بستگی دارد. در این دسته از الگوریتم ها علاوه بر انتقال پیام رمز شده, کلید مورد استفاده نیز می باید در مقصد موجود بوده و یا به نحوی به مقصد انتقال یابد. برخی از الگوریتم های رمزنگاری متقارن به شرح زیر است:

الف- DES

ب – DES3

ج- AES

الگوریتم های رمز نامتقارن: یکی از مسائلی که در رمزنگاری به آن برخورد میشود نحوه انتقال کلید از مبدا به مقصد می باشد. در الگوریتم های متقارن پیام را با استفاده از کلید مشترک رمز نموده و از مبدا به مقصد ارسال می نمائیم. در برخی از مواقع نیاز است کلید مورد استفاده به همراه پیام رمز شده از مبدا به مقصد ارسال شود . این امر نیازمند راهکاری مجزا برای ارسال کلید از مبدا به مقصد می باشد.

به طور معمول در الگوریتم های رمز نا متقارن از دو کلید برای عملیات رمزنگاری استفاده می شود. متن اولیه در مبدا با استفاده از کلید عمومی رمز شده و در مقصد با استفاده از کلید اختصاصی گشوده خواهد شد. الگوریتم های نا متقارن به طور عمده برای ارسال کلید مورد استفاده قرار میگیرند. با اینحال در برخی از مواقع ممکن است این الگوریتم برای رمز نگاری داده ها نیز استفاده شوند.

امنیت الگوریتم های رمزنگاری نا متقارن به نحوه انتخاب و طول کلید بستگی دارد و این امر نیازمند محاسبات و پردازش های لازم برای ایجاد کلید و انتخاب آن خواهد بود. با افزایش طول کلید محاسبات مورد نیاز برای رمزنگاری افزایش یافته که این امر موجب افزایش نیاز به منابع سخت افزاری بوده و با کاهش طول کلید ضریب امنیت سیستم کاهش خواهد یافت. برخی از الگوریتم های رمزنگاری نا متقارن به شرح زیر است:

الف- RSA

ب- ECC

ج - DSA

د - Diffie-Hellman

ه - ELGamal

۲- الگوریتم های رمز نگاری و رمز گشایی موجود :

۲-۱ : الگوریتم های رمزنگاری با کلید متقارن :

۲-۱-۱: DES :

به دنبال فراخوان موسسه دفتر ملی استاندارد امریکا که در سال ۱۹۷۳ انتشار یافت پروپوزالی مبنی بر درخواست طراحی یک سیستم رمزنگاری ارائه شد. درواقع این مساله به عنوان نقطه عطفی در تاریخ رمزنگاری به حساب می اید که این علم را از هویت یک هنر سیاه و بعنوان ابزاری که الزاما برای مقاصد نظامی و امنیت ملی کاربرد دارد خارج ساخت. دفتر ملی استاندارد امریکا تشخیص داد که میتوان از الگوریتم های رمزنگاری برای توسعه امنیت شبکه های ارتباطی کامپیوتری استفاده نمود.

به این فراخوان پاسخی داده نشد تا اینکه در فراخوان دوم شرکت IBM به توسعه الگوریتم رمزنگاری مورد نظر همت گماشت تا انکه الگوریتم طراحی شده توسط این شرکت توسط آژانس امنیت ملی در سال ۱۹۷۵ انتشار یافته و پس از بحث و مشاوره در سال ۱۹۷۶ توسط دفتر ملی استاندارد امریکا پذیرفته شده و در سال ۱۹۷۶ به عنوان الگوریتم DES انتشار یافت.

استفاده از الگوریتم DES در سال ۱۹۷۷ برای آژانس های فدرال الزامی شد و پس از انطباق ان با الگوریتم بانکی ANSI X3.92 به صورت گسترده ای در صنایع تجاری مورد استفاده قرار گرفت. در واقع استاندارد DES به صورت بالقوه به عنوان استاندارد بین المللی رمزنگاری در صنایع شناخته شد. وضعیتی که تا زمان معرفی الگوریتم AES پایدار ماند. اگرچه پیش بینی شد الگوریتم DES چرخه عمر برابر ۱۵ سال داشته باشد ولی آژانس امنیت ملی در سال ۱۹۸۸ تائیدیه آن را حذف نمود. با این همه دفتر ملی استاندارد امریکا تائید اعتبار آن را در همان سال انجام داد. دفتر ملی استاندارد که اکنون به عنوان موسسه ملی استاندارد و تکنولوژی شناخته می شود.عدم انطباق این الگوریتم را اعلام نمود که این مساله موجب فراخوان دومی برای الگوریتم های رمزنگاری در سال ۱۹۹۸ شد.

بر اساس مستند شماره fips46-3 الگوریتم رمزنگاری DES در ۲۵ اکتبر سال ۱۹۹۹ مورد تائید قرار گرفت و در تاریخ ۱۹ می ۲۰۰۵ از دور خارج شد.

۲-۱-۲ : DES3 :

با توجه به نقاط ضعف الگوریتم DES و لزوم تقویت ان الگوریتم DES۳ معرفی شد. الگوریتم DES۳ بر مبنای الگوریتم DES طراحی شده است. وجه تمایز الگوریتم DES۳ در اجرای سه مرحله ای آن می باشد. این الگوریتم از سه کلید مجزا برای رمزنگاری استفاده میکند. فرایند های رمزنگاری و رمزگشایی در این روش به شرح زیر می باشد.

فرایند رمزنگاری:

$$O=Ek3(Dk2(Ek1(I)))$$

۱- متن مورد نظر بوسیه الگوریتم DES و کلید k1 رمزنگاری می شود.

۲ - خروجی مرحله اول توسط کلید k2 رمزگشایی می شود

۳ - خروجی مرحله دوم توسط کلید k3 مجددا رمزنگاری میشود.

فرایند رمزگشایی:

I=Dk1(Ek2(Dk3(O)))

۱ - متن رمزشده توسط کلید k3 رمزگشایی میشود.

۲ - خروجی مرحله اول توسط کلید k2 رمزنگاری می شود.

۳ - خروجی مرحله دوم توسط کلید k1 رمزنگاری می شود.

خروجی مرحله سوم به عنوان متن اولیه قابل استفاده خواهد بود. با کمی بررسی مشاهده می شود فرایند رمزگشایی قرینه فرایند رمزنگاری می باشد.

مستند FIPS46-3 ترکیب پیشنهادی زیر را برای انتخاب کلیدهای K1, K2, K3 ارائه می دهد:

۱ - K1, K2, K3 مستقل از همدیگر انتخاب شوند.

۲ - K1, K2 بطور مستقل از هم انتخاب شده و K1=K3 باشد.

۳- K1=K2=K3

۳-۱-۲: AES :

الگوریتم رمزنگاری AES به منظور جایگزینی با الگوریتم رمزنگاری DES توسعه یافت .موسسه فدرال پردازش استاندارد اطلاعات (FIPSنسخه خاصی از الگوریتم مورد نظر را برای استفاده سازمان های دولتی انتشار داد. با اینهمه الگوریتم AES به طور گسترده ای توسط سازمانهای دولتی, موسسات تحقیقاتی و سازمانهای غیر دولتی مورد استفاده قرار گرفت.

دو محقق بلژیکی در حوزه رمزنگاری به نام های دکتر ژان دایمن از موسسه بین المللی دنیای پروتون و دکتر وینسنت ریجمن دارای مدرک پست دکتری, محقق دپارتمان مهندسی برق دانشگاه کاتولیک لئووین, طراحان این الگوریتم می باشند.

موسسه ملی استاندارد و تکنولوژی این الگوریتم را به دلیل داشتن ترکیبی از امنیت, عملکرد, تاثیر پذیری, سهولت پیاده سازی و سادگی انتخاب نمود. به وضوح این الگوریتم, عملکرد بسیار خوبی در استفاده از سخت افزار و نرم افزار در طیف وسیعی از محیط های محاسباتی از خود نشان داده است.

حافظه بسیار کم مورد نیاز برای این الگوریتم استفاده از ان را برای ابزارهای محاسباتی که دارای محدودیت فضای حافظه هستند بسیار مناسب نشان میدهد. این الگوریتم عملکرد مناسبی در مقابل حمله منبع مصرفی و حمله بازه زمانی از خود نشان میدهد. علاوه بر آن مشخص است برخی از عملیات دفاعی را می توان بر روی این الگوریتم اعمال نمود بدون آنکه بر عملکرد الگوریتم تاثیر گذار باشد. درنهایت چرخه های داخلی الگوریتم مشخص میکند که این الگوریتم پتانسیل خاصی در اجرای موازی دستورالعمل ها دارا می باشد. الگوریتم AES از سه کلید در اندازه های ۱۲۸,۱۹۲ و ۲۵۶ بیتی استفاده می کند [۱].

پیشنهاد طراحی الگوریتم AES :در سال ۱۹۹۸ موسسه ملی استاندارد و تکنولوژی فراخوانی را برای طراحی یک الگوریتم رمزنگاری پیشنهاد نمود . در این پیشنهاد سه خصوصیت اصلی بعنوان نیازمندی های الگوریتم رمزنگاری جدید ارائه شد که به شرح زیر است:

۱ - سایز بلاک مورد استفاده می بایست ۱۲۸ بیت باشد.

۲ - برای بلاک پیشنهادی رمز شده می بایست بتوان طراحی بر اساس ۱۲۸, ۱۹۲ و ۲۵۶ بیت پیاده سازی نمود. به بیان دیگر به توسعه دهندگان آتی می بایست امکان انجام اقدامات برای جستجوی جامع را ارائه داد. چنین جستجویی دقیقا وابسته به قابلیت تکنیکهای جستجوی تمام کلید خواهد داشت.

۳ - بلاک رمز شده می بایست قابلیت پردازش سریع تری نسبت به الگوریتم رمزنگاری DES۳ بر روی پلتفرم های متفاوت داشته باشد.

به وضوح و با توجه به توسعه الگوریتم DES چنین مشخصه ای وجود یک رقابت را برای انتخاب یک الگوریتم و دسترسی به جزئیات طراحی الگوریتم رمزنگاری به رایگان تعیین میکند.

۲-۲: الگوریتم های رمزنگاری با کلید نا متقارن :

۲-۲-۱ : RSA :

الگوریتم RSA نام خود را از ابتدای نام ابداع کنندگان خود برگرفته است این الگوریتم از دو کلید عمومی و اختصاصی برای فرایند رمزنگاری استفاده می کند . از کلید عمومی برای رمزنگاری پیام و از کلید اختصاصی برای رمزگشایی پیام استفاده میشود. در این روش از سه الگوریتم به شرح زیر در فرایند رمزنگاری استفاده میشود:

- الگوریتم تولید کلید

- الگوریتم رمزنگاری

- الگوریتم رمزگشائی

برای رمز نگاری به روش RSA ابتدا به صورت زیر عمل میشود

مرحله اول تولید کلید: برای تولید کلید اقدامات زیر را انجام میدهیم

- دو عدد p و q را انتخاب میکنیم به گونه ای که نسبت به هم اول باشند

- مقادیر n و ø را بر اساس فرمول زیر محاسبه میکنیم

$$n = pq$$

$$ø= (p - 1)(q - 1)$$

- عدد تصادفی e را به گونه ای ایجاد کنید که شرایط زیر برقرار باشد.

$ø < e < ۱$

$gcd(e; ø) = 1$

- از الگوریتم توسعه یافته اقلیدسی برای محاسبه d استفاده کنید به گونه ای که شرایط زیر برقرار باشد

$ø < d < ۱$

$ed \equiv 1 (mod\ ø)$

- در این مرحله (n ,e)بعنوان کلید عمومی و d به عنوان کلید اختصاصی معرفی می شود.

الگوریتم رمزنگاری RSA: این الگوریتم پس از تولید کلید و برای رمزنگاری و رمزگشایی داده مورد استفاده قرار می گیرد جزئیات این الگوریتم به شرح زیر است.

رمزنگاری :

- ابتدا کلید های عمومی (n ,e)طرف مقابل اخذ می شود

- پیام مورد نظر به اعداد بین صفر تا i-1 تبدیل می شود

- هر عدد بدست آمده با فرمول $c=(i^e) \bmod n$ رمزنگاری می شود

- مقدار c به عنوان پیام برای طرف مقابل ارسال می شود

رمز گشایی :

پیام به کمک کلید اختصاصی $m=(c^d) \bmod n$ رمز گشایی می شود

۲-۲-۲: Diffie–Hellman

یکی از مسائل قابل توجه در رمزنگاری نحوه توزیع کلید می باشد. کلیدهای ایجاد شده می بایست به نحوی بین مبدا و مقصد رد و بدل شوند و این دسترسی می بایست به نحوی انجام شود که کلید مورد نظر توسط افراد بدون صلاحیت قابل دسترسی و بهره برداری نباشد. نحوه ارسال کلید نیز میتواند به نحوی توسط فرایند رمزنگاری و یا انجام برخی از محاسبات انجام پذیرد. الگوریتم دیفی هیلمن از این قاعده مستثنی نبوده و با انجام محاسبات لازم ارسال کلید بین مبدا و مقصد را امکان پذیر می سازد.

این الگوریتم توسط Whitefield Diffie و Martin Hellman در سال ۱۹۷۶ ابداع شد. این الگوریتم میتواند برای ارسال کلید از یک کانال عمومی استفاده کند که نیاز به هیچگونه محدودیتی در استفاده از آن نیست و این کانال میتواند برای عموم قابل دسترس باشد. این کانال برای عموم قابل شنود بوده و انتقال کلید براساس انجام محاسبات بین مبدا و مقصد می باشد.

در مورد این الگوریتم میتوان گفت :(martin)

۱ - کلید های عمومی و اختصاصی کاربران با زوج (P,S) شناخته میشود که میتواند موقتی باشد.

۲ - برای رمزنگاری از تابع F استفاده میگردد که به ازاء دو ورودی x, y خروجی مورد نظر را به صورت F(x,y) تولید کند.

ساختار کلی رمزنگاری در الگوریتم دیفی هیلمن به شرح زیر است.

۱ - آلیس کلید عمومی خود را برای باب ارسال میکند.

۲ - باب کلید عمومی خود را برای الیس ارسال میکند

۳ - آلیس تابع F(Sa,Pa) را محاسبه میکند. الیس زمانی میتواند این کار را انجام دهد که کلید اختصاصی Sa را در اختیار داشته باشد.

۴ - باب تابع F(Sb,Pb) را محاسبه میکند. باب زمانی میتواند این کار را انجام دهد که کلید اختصاصی Sb را در اختیار داشته باشد.

خصوصیت اساسی این سیستم رمزنگاری کلید عمومی را میتوان در تابع زیر عنوان نمود

$$F(Sa,Pb) = F(Sb,Pa)$$

این خصوصیت موجب می شود بر اساس محاسبه انجام شده ,کلید های بدست امده برای طرفین دارای مقداری یکسان باشد.

رمزنگاری به روش Diffie–Hellman

الگوریتم رمزنگاری را میتوان به شرح زیر عنوان نمود:

۱ - آلیس و باب بر روی عدد اول بزرگ p,g توافق میکنند که عدد p بسیار بزرگ خواهد بود. نیازی نیست که این دو عدد مخفی نگه داشته شوند.

۲ - آلیس و باب دو عدد اول Xa , Xb را به صورت تصادفی انتخاب می کنند که کوچکتر از p می باشند. این دو عدد به عنوان کلید خصوصی می باید مخفی نگه داشته شوند.

۳ - آلیس کلید قابل ارسال را با استفاده از فرمول Ya= (g^Xa) mod p و بطور مشابه باب کلید قابل ارسال را با استفاده از فرمول Yb= (g^Xb) mod p محاسبه میکند . اعداد بدست آمده از طریق یک کانال ناامن برای طرفین ارسال خواهد شد.

۴ - آلیس کلید مورد نظر را با استفاده از فرمول Za= (Yb^Xa) mod p و به طور مشابه باب با استفاده از فرمول

Zb=(Ya^Xb) mod p کلید مورد نظر را استخراج میکند.

۵ - Za = Zb کلید مشترک محسوب شده و برای عملیات رمزنگاری متقارن قابل استفاده می باشد.

(عملگر ^ به معنی توان رساندن می باشد)

۳-۲-۲: ELGamal :

الگوریتم ELGamal توسط رمز نگار مصری طاهر الجمال طراحی شده است. این الگوریتم بنام طراح آن نامگذاری شده و از نوع نامتقارن می باشد. در این الگوریتم از کلید عمومی برای رمزنگاری و از کلید اختصاصی برای گشودن پیام رمز شده استفاده می شود.

خصوصیت این الگوریتم به گونه ای است که در هر مرحله از فرایند رمزنگاری یک کلید تصادفی k تولید میشود مقدار این کلید کاملا تصادفی بوده و در هر مرحله از اجرای فرایند رمز نگاری کلید تولید شده با کلید قبلی متفاوت خواهد بود.

این خصوصیت موجب میشود در دو مرحله متفاوت خروجی متفاوت تولید شود, که این خصوصیت از ویژگی های تولید کلید K در هر مرحله از فرایند رمزنگاری می باشد .فرایند تولید تصادفی کلید K موجب می شود حدس زدن کلید K از روی مقدار C1 امکان پذیر نباشد.

در سیستم رمزنگاری ElGamal فرایند رمزنگاری بر اساس دو الگوریتم زیر انجام می شود

•الگوریتم تولید کلید

•الگوریتم رمزنگاری

الگوریتم تولید کلید:

موجودیت A برای رمزنگاری اقدامات زیر را انجام می دهد:

- ابتدا یک عدد بزرگ p انتخاب میگردد. بهتر است بین ۱۰۲۴ الی ۲۰۴۸ بیت باشد .

- عدد ویژه g انتخاب شده که می بایست نسبت به p اول بوده و در بازه ۱, (p-1) قرار داشته باشد کلید تصادفی x که عددی بین ۱, (p-1) است انتخاب شود. هر کاربر سیستم می بایست کلید مستقل خود را داشته باشد

- کلید عمومی با فرمول $y=g \wedge x \bmod p$ محاسبه شود

- مقادیر (p, g, y) به عنوان پارامترهای سیستم ارائه شود

الگوریتم رمزنگاری:

- موجودیت B پیام m را برای A به صورت زیر رمز می کند

- عدد k را به صورت تصادفی تولید می کند.

- رشته P را که به مقدار عددی تبدیل شده است با فرمول زیر به رمز تبدیل می کند

$C\_1=g\wedge k \bmod p$

$C\_2=Py\wedge k \bmod p$

-مقدار $C=(C_1,C_2)$ را به عنوان پیام رمز شده به مقصد ارسال می کند پیام قابل ارسال بر اساس فرمول بالا اماده سازی شده و به مقصد ارسال می شود. مقدار k در هر مرحله از فرایند رمزنگاری متفاوت است بنابراین یک متن ثابت در این روش میتواند به اشکال متفاوت رمز شود.

الگوریتم رمزگشایی:

برای رمزگشایی به روش زیر عمل می کنیم:

از فرمول $P=C_2/((C_1)^x \bmod p)$ برای استخراج مقدار عددی P استفاده می کنیم مقدار عددی Pرا به رشته مورد نظر تبدیل می کنیم

۳- الگوریتم پیشنهادی :

۳-۱ : الگوریتم $FR1$:

الگوریتمی است که توسط رضا رصاف بخش بعد از گذشت ۲ سال و در سال ۲۰۱۸ میلادی طراحی و پیاده سازی شد که ایده این الگوریتم با توجه به الگوریتم های موجود و بهینه سازی بیشتر انجام شد که البته در این اینجا به جزئیات و خصوصیات بیشتر این الگوریتم می پردازم.

در ابتدا باید به این نکته اشاره کنم این الگوریتم بصورت کاملا پویا ایجاد شده است. که البته در ورژن اولیه خود می باشد . بعد از طراحی و پیاده سازی در شرایط و سیستم های مختلف شبیه سازی شده است و در نهایت با توجه به پویایی و عدم ایستا بودن فرمول های بکار رفته ، شکستن داده های کد شده زمانبر تر شده نسبت به الگوریتم های موجود در دنیای شبکه و اینترنت.

نکته قابل توجه اینکه الگوریتم از فرمول های متعددی در زمان کد کردن داده ها استفاده میکند ، و هر داده را با یک نوع الگوی خاص کد گذاری نموده و ارسال می نماید. و در نهایت با توجه به اِلمان های بسته ارسالی کار تجزیه و تحلیل پکت انجام میشود که عملیات رمزگشایی صورت پذیرد و داده های اولیه به سلامت در مقصد به نمایش بیاید.

الگوریتم $FR1$ کلید اصلی را در بسته نهایی پس از رمزنگاری بر روی کلید اصلی ، آن را در بسته ارسالی قرارداده و ارسال می نماید .

دو مرحله از امنیت بالا میرود . چراکه در مرحله اول کلید اصلی کد گذاری شده و دسترسی به کلید اصلی هم سخت و دشوار خواهد شد و در مرحله دوم کلید اصلی در لابه لای بسته ارسالی جاسازی شده و انتقال داده میشود این هم خود دلیلی بر امنیت بالاتر نسبت به بقیه الگوریتم ها می باشد .

الگوریتم طراحی شده برای هر بسته ، عملوند ها و عملگر های تصادفی انتخاب خواهد کرد و حتی اگر یک بسته در احتمال بسیار پایین (بدست هکر ها) افتاد ، رمزگشایی بسته های بعدی غیر ممکن خواهد شد و با روش قبلی نمیتوان آنرا از رمز خارج کرد .

۳-۲ : مزایای الگوریتم FR1

۱ – الگوریتم کامل پویا می باشد .

۲- الگوریتم کلید اصلی را هم به صورت کد شده تبدیل می نماید .

۳- الگوریتم در هر بار اجرا یک کد تولید کرده و کد ایستا ندارد و در هر مرحله اجرا فرمول جدیدی تولید میکند.

۴ - الگوریتم کلید اصلی را به همراه بسته کد شده ارسال می نماید . که اینکار باعث میشود داده اولیه و کلید اصلی هیچکدام در دسترس قرار نگیرد و عملیات اصلی از دست داده نشود.

۵ - این الگوریتم پیچیدگی خاصی ندارد و زمان اجرای آن از تابع O(n) پیروی میکند و باعث افزایش سرعت الگوریتم می شود.

۶- در اینجا هر کدام از بسته ارسالی داده هم (هکرها) بدست بیاورند به هیچ عنوان قادر به تشخیص عملیات کد گذاری نخواهند بود چراکه عملیات اجرا شده بر روی داده اولیه به صورت داینامیک رخ می دهد و همین امر باعث افزایش امنیت داده ها در ارسال بسته ها می شود.

۴- نتیجه گیری :

محاسبات ابری آخرین پیشرفتی است که دسترسی آسان به منابع محاسباتی بدون نصب نرم افزار را ارایه میدهد. محاسبات ابری منافع زیادی برای کاربرانش دارد اما از بعضی تهدیدات امنیتی رنج میبرد. امنیت داده یکی از مهمترین موانع برای رشد این تکنولوژی می باشد. در این پایان نامه استفاده از تکنیک های رمزنگاری در حوزه محاسبات ابری بررسی شده است .

DES 1، DES، AES و Blowfish از الگوریتم های کلید متقارن می باشند. DES و AES الگوریتم های کلید متقارنی هستند که بیشترین استفاده را در محیط ابر دارند، DES نسب به AES پیاده سازی راحت تری دارد.

الگوریتم های RSA و تبادل کلید دیف هلمن از الگوریتم های کلید نا متقارن هستند. در محاسبات ابری هر دوی این الگوریتم ها ، برای تولید کلید رمزنگاری برای الگوریتم های کلید متقارن استفاده می شوند.

اما الگوریتم های رمزنگاری که اجازه عملیات هایی مثل جستجو کردن روی داده های رمزگشایی شده را میدهند، برای محاسبات ابری موردنیاز هستند که در این صورت محرمانگی داده نیز حفظ خواهد شد.

الگوریتم پیشنهادی FR1 که دراین پایان نامه ارائه شده است میتوان استفاده های فراوانی کرد ، چرا که کاملا پویا هست و امنیت بالاتری نسبت به بقیه الگوریتم ها دارد. دلایل گفته شده در فصل ۴ گویای این موضوع است . این الگوریتم که به تازگی طراحی و پیاده سازی شده است توانایی انجام رمزنگاری های متعدد الگو های داینامیک می باشد که بیش از ۶۰۰۰ حالت ممکن در ورژن اولیه خود قرار داده است .

منابع فارسی :

۱. اسدنجفی، نرگس و ملامطلبی، مهدی،۱۳۹۹،بهبود احراز هویت در خانه هوشمند مبتنی بر رمز یکبار مصرف و رمزنگاری منحنی بیضوی، فصلنامه علوم و فناوری های پدافند نوین، دوره: ۱۱، شماره: ۴ ،https://civilica.com/doc/1184755

۲. امینی آذر، وهاب و فرحی، رسول و دشتی، فاطمه،۱۴۰۲،ارائه یک راهکار رمزنگاری سبک وزن به منظور تامین امنیت داده در اینترنت اشیا،دوفصلنامه فناوری اطلاعات و ارتباطات ایران، دوره: ۱۶، شماره: ۶۱ ،https://civilica.com/doc/2137614

۳. بهروزیان، میثم،۱۴۰۴،چارچوب ترکیبی یادگیری فدرال و رمزنگاری منحنی بیضوی برای تشخیص ناهنجاری در شبکه های اینترنت اشیاء با تضمین حریم خصوصی و کارایی بهینه،https://civilica.com/doc/2409777

۴. حکمتیان، ایران،۱۳۹۶،طراحی یک سیستم بازیابی اطلاعات محرمانه مبتیی بر رمزنگاری می‌حنی بیضوی،نخستین کنفرانس ملی پیشرفت ها و فرصت های فناوری اطلاعات و ارتباطات،تهران،https://civilica.com/doc/781781

۵. حمیدزاده، جواد و ابوالفتح زاده امینجان، محمود و زرقانی، محمد،۱۳۹۴،استفاده از منطق فازی در فرآیند رمزنگاری و رمزگشایی اطلاعات بر رویGPU ،چهاردهمین کنفرانس سیستم های فازی ایران،تبریز،https://civilica.com/doc/730921

۶. رصاف بخش ، رضا ، ۱۳۹۶ ، بررسی تهدیدات فناوری اطلاعات (IT) و راه های مقابله با حملات جهت بهبود امنیت شبکه های کامپیوتری ، سومین کنفرانس بین المللی پژوهش در علوم و تکنولوژی ، آلمان

۷. رضایی ادریانی، سجاد و سجادیه، مهدی،۱۴۰۱،رای گیری الکترونیکی بر اساس رمزنگاری همریخت در گروه خم بیضوی، مجله فناوری های نوین مهندسی برق در سیستم انرژی سبز، دوره: ۱، شماره: ۳ ،https://civilica.com/doc/1535501

۸. رمضانی، فاطمه و چمکوری، علیرضا،۱۴۰۴،بهبود امنیت داده در رایانش ابری عمومی با استفاده از یک معماری ترکیبی مبتنی ECC, AES،دومین کنفرانس ملی علم داده در کاربردهای مهندسی،تبریز،https://civilica.com/doc/2459124

۹. سلطانی، ایمان و مختاری، شیوا،۱۳۹۸،الگوریتم رمزنگاریAES ،ششمین کنگره ملی تازه های مهندسی برق و کامپیوتر ایران با نگاه کاربردی بر انرژی های نو،تهران،https://civilica.com/doc/923878

۱۰. سیادتیان، سیدمهدی و فراهی، احمد،۱۴۰۰،مروری بر روشهای رمزنگاری پایگاه داده های ابری،چهارمین کنفرانس بین المللی مهندسی برق، کامپیوتر و مکانیک،تهران،https://civilica.com/doc/1271653

۱۱. شاعری نیا، رضا و حسینی، سید اکبر و حاجیان، رحمان و عرفانی، سیدحسین،۱۴۰۴،ارائه یک طرح احراز هویت و توافق کلید ایمن و کارا مبتنی بر رمزنگاری منحنی بیضوی برای محیط های اینترنت اشیاء صنعتی،نخستین همایش ملی "هوش مصنوعی و پژوهش های نوظهور:همگرایی انسان و سیستم های هوشمند،تهران،https://civilica.com/doc/2323300

۱۲. شریفی، محمدعلی و پارسا، حسین و سیاح مقدم، امین،۱۴۰۳،بهبود الگوریتم های رمزنگاری با سیستم تراختنبرگ مطالعه ای درباره سرعت و امنیت،سومین کنفرانس بین المللی پژوهش در ریاضیات، فیزیک و محاسبات عددی،تهران،https://civilica.com/doc/2191132

۱۳. شفارودی، رضا،۱۴۰۳،ساختارهای جبری در رمزنگاری پست کوانتومی،اولین همایش بین المللی معلمان استعدادیاب و فرهنگ ساز در توسعه آموزش های فنی و حرفه ای و کاردانش در مسیر توسعه پایدار،https://civilica.com/doc/2227400

۱۴. عطایی نژاد، مریم و براتی، حمید،۱۳۹۸،یک روش احرازهویت دوطرفه مبتنی بر رمزنگاری منحنی بیضوی در سیستم رادیوشناسه،سومین کنفرانس ملی کامپیوتر، فناوری اطلاعات و کاربردهای هوش مصنوعی،اهواز،https://civilica.com/doc/1015586

۱۵. عماد، فرزانه،۱۴۰۳،بهبود روشهای تضمین امنیت داده با استفاده از مکانیزمهای کنترل دسترسی در رایانش ابری،هفتمین همایش ملی فناوریهای نوین در مهندسی برق، کامپیوتر و مکانیک ایران،تهران،https://civilica.com/doc/2050311

۱۶. کشاورزی، پرویز و جعفری، محبوبه،۱۳۹۷،افزایش سرعت پیاده سازی سخت افزاری در رمزنگاری منحنی بیضوی در میدان محدود اول،اولین کنفرانس ملی مهندسی برق، کامپیوتر و فناوری ارتباطات،اصفهان،https://civilica.com/doc/936173

۱۷. نوری، داود و یغمایی مقدم، محمدحسین و نیکوقدم، مرتضی،۱۳۹۲،مدیریت کلید با استفاده از رمزنگاری منحنی بیضوی برای خوشه بندی امن در شبکه های حسگر بیسیم،دهمین کنفرانس بین المللی انجمن رمز ایران،یزد،https://civilica.com/doc/788029

۱۸. نیک خواه، حسین،۱۳۹۷،افزایش امنیت و کاهش مصرف انرژی در شبکه حسگر بی سیم با استفاده از رمزنگاری منحنی بیضوی،دومین همایش بین المللی مهندسی برق،علوم کامپیوتر و فناوری اطلاعات،همدان،https://civilica.com/doc/766403

۱۹. همتی، سارا و تقی پورعیوضی، شیوا،۱۳۹۵،بررسی انواع روش و الگوریتم های رمزنگاری،اولین مسابقه کنفرانس بین المللی جامع علوم مهندسی در ایران،بندرانزلی،https://civilica.com/doc/545454

منابع انگلیسی :

1. Abbas, S.U. Khan, A review on the state-of-the-art privacy preserving approaches in e-health clouds, IEEE J. Biomed. Health Inform. (2014), http:// dx.doi.org/10.1109/JBHI.2014.2300846.

2. S.Srividhya and Dr. R.Rathinasabapathy, "VIRTUALIZATION SECURITY IN CLOUD COMPUTING" , shanlaxjournals , 2015 ,vol 3 , no.1 ,pn 48,

3.Bhavana Agrawal, Himani Agrawal, Monisha Mishra(2013),"Implementation of Various Cryptosystem Using Chaos"IOSR Journal of Computer Engineering (International Organization of Scientific Research)

4.Detection in the Cloud via Side-Channel Analysis". In Proceedings of IEEE Computer Society: 2011 IEEE Symposium on Security and Privacy, DOI 10.1109/SP.2011.31.

6.Thomas Ristenpart, EranTromer, HovavShacham, Stefan (2009) " Hey,You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds" . Savage Attack on Amazon EC2 web services. Dept. of Computer Science and Engineering University of California, San Diego, USA.

7.Adel A. El-Zoghabi, Amr H. Yassin, Hany H. Hussien (2013)," Survey Report on Chaos Based Public-key Cryptosystem". International Journal of Emerging Technology and Advanced Engineering.

8.BhruguSevak (2012),"Security against Side Channel Attack in Cloud Computing". International Journal of Engineering and Advanced Technology (IJEAT).

9.Kashish Goyal,Supriya Kinger "Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications(0916-4441)Volume 11-No.1.July 2011.

10. Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 01, Oct 2011.

11. Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 6, August 2011.

12. D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 4, 2009.

Securing cloud computing computer networks using dynamic encryption algorithm FR1

Mohammad Hadinia
Master's degree in Information Technology Engineering, Security and Information, Imam Reza International University (PBUH)

Abstract— Cryptography is the science that studies and understands the principles and methods of transferring or storing information securely, even if the information transfer path and communication channels or the information storage location are insecure. Cloud computing is one of the emerging technological opportunities that has been able to significantly reduce the need to purchase specialized hardware and, as a result, the related costs for users. One of the important parts of cloud computing is cloud storage. The significant reduction in costs and high processing speed in cloud storage have made cloud databases very popular among various businesses. But on the other hand, cloud databases face serious security challenges. This issue illustrates the importance of trying to improve the security of cloud databases. One of the popular methods in this field is encryption. In this article, the security of cloud computing virtualization using symmetric and asymmetric keys will be examined, and as a result, a dynamic algorithm called FR1 has been designed and simulated, which will increase security many times and prevent hacking of encrypted information.

Keywords: Encryption and decryption, computer networks, cloud computing