9th SASTech Symposium on Advances in Science & Technology (2014)
نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
بامحوریت
امنیت ملی و توسعه پایدار
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

ارائه یک روش جدید در ارسال پیام و ذخیره سازی داده در محیط ابر با استفاده از توسعه الگوریتم استاندارد رمزنگاری AES

ناصر عطار

دانشجوی کارشناسی ارشد ،دانشگاه غیرانتفاعی سلمان – مشهد

Naser.Attar@Yahoo.com

ارائه دهنده : ناصر عطار

چکیده

رمزنگاری علم کدها و رمزها است. یک هنر قدیمی است و برای قرنها به منظور محافظت از پیغامهایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل می‌شده، استفاده شده است تا پیغامهای آنها محرمانه بماند. هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند. امروزه رایانش ابری مزیتهای زیادی را به دنبال داشته ، و همچنان در حال رشد و توسعه می باشد. اما با وجود این مزیتها با چالش بزرگی مثل امنیت روبه رو است . در این مقاله سعی داریم با توسعه الگوریتم رمزنگاری AES به عنوان یک رویکرد جدید ، امنیت داده ها در ابر را حفظ کنیم .

کلمات کلیدی-داده - پردازش ابری - توسعه الگوریتم رمز نگاری AES - امنیت – الگوریتم های رمزنگاری

۱– مقدمه:

رمزنگاری مخفف‌ها و اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از دیتای اصلی ، آنرا با استفاده از یک کلید (رشته‌ای محدود از بیتها) بصورت رمز در می‌آوریم تا کسی که دیتای حاصله را می‌خواند قادر به درک آن نباشد. دیتای رمزشده که بصورت یک سری از بیتها بدون داشتن رابطه مشخصی با دیتای اصلی بنظر می‌رسد. برای به دست آوردن متن اولیه ، دریافت‌کننده آنرا رمزگشایی می‌کند. یک شخص ثالث (مثلا یک هکر) می‌تواند برای اینکه بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمزنوشته کند. بخاطرداشتن وجود این شخص ثالث ، الگوریتم رمزنگاری بسیار مهم است.رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده‌اند. کلید، یک رشته از ارقام دودویی (صفر و یک) است که بخودی‌خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند[۱و۲] در این مقاله ما سعی داریم کلید الگوریتم AES را پیچیده تر تولید کنیم، تا در مقابل حملات در ابر مقاوم باشد . در ادامه کارهای مرتبط در بخش دوم و اهمیت موضوع امنیت در ابر در بخش سوم بیان شده است . در بخش چهارم انواع حملات در ابر بررسی می شود و در بخش پنجم الگوریتم استاندارد AES توضیح داده خواهد شد ودر بخش ششم رویکرد پیشنهادی مطرح می شود ودر بخش بعدی مقایسه روش پیشنهادی با دیگر روشها انجام خواهد گرفت و درنهایت نتیجه گیری از کل مقاله ارائه خواهد شد.

۲- کارهای مرتبط

در امنیت ابر از تکنیک های خاصی برای حفاظت از داده ها انجام شده است که مروری بر آنها خواهیم داشت.

۲-۱ – استفاده از سیاستهای امنیتی در ابر

استفاده از سیاستهای امنیتی در واقع مدیریت ریسکهای امنیتی در ابر می باشد که می تواند شامل، استفاده از تیم های امنیتی متخصص ، مدیریت و بازسازی آسیب پذیری ، به روز رسانی بسته های نرم افزاری و سیستم عامل ها و استفاده از اتصالات ایمن باشد. سیستم های تشخیص نفوذ برای جلوگیری از حملات می تواند موثر باشد. [۲]

۲-۲- استفاده از الگوریتم های رمزنگاری