

رمزنگاری MD5 جهت امنیت در محاسبات ابری

مؤلف:

مهندس آیدان قجقی

دکتر میر سعید حسینی شیروانی

سرشناسه	فجقی، آیدان، ۱۳۶۵ -
عنوان و نام پدیدآور	رمزنگاری MD5 جهت امنیت در محاسبات ابری / مولف آیدان فجقی، میر سعید حسینی شیروانی
مشخصات نشر	گرگان: انتشارات نوروزی، ۱۳۹۶.
مشخصات ظاهری	۱۲۰ص: مصور، جدول.
شابک	978-600-449-325-3
وضعیت فهرست نویسی	فیا
یادداشت	کتابنامه
موضوع	محاسبات ابری Cloud computing
موضوع	محاسبات ابری -- تدابیر ایمنی Cloud computing-- Security measures
موضوع	وب -- خدمات Web services
موضوع	نرم افزار کاربردی Application software
موضوع	داده پرداز Electronic data processing
شماره افزوده	حسینی شیروانی، میر سعید، ۱۳۵۷ -
رده بندی کنگره	Q۸۵۸۵/۷۴/۳۸ ۱۰۶
رده بندی دیویی	۶۷۰۶
شماره کتابشناسی ملی	۴۷۰۴۸

رمزنگاری MD5 جهت امنیت در محاسبات ابری

تألیف: مهندس آیدان فجقی - دکتر میر سعید حسینی شیروانی

صفحه آرا و طراح جلد: بهاره عزت تبار

نوبت چاپ: اول- ۱۳۹۶

مشخصات ظاهری: ۱۲۲ ص

قطع: وزیری

شمارگان: ۳۰۰

شماره شابک: ۳-۳۲۵-۴۴۹-۶۰۰-۹۷۸

چاپ و نشر: نوروزی-۱۷۳۲۲۴۲۲۵۸

قیمت: ۱۱۰۰۰ تومان

حق چاپ برای نویسنده محفوظ می باشد.



نشانی: گلستان، مگرگان، خیابان شهید بهشتی، بازار رضا(ع)، ۰۱۷-۳۲۲۴۲۲۵۸

دورنگار: ۰۱۷-۳۲۲۲۰۰۴۷ آدرس الکترونیکی: Entesharate.noruzi@gmail

سایت انتشارات: www.Entesharate-noruzi.com

فهرست مطالب

۱۳	پیشگفتار
۱۵	فصل اول: مقدمه
۱۶	مقدمه
۱۸	اهمیت موضوع
۱۹	مثله
۲۱	فصل دوم: محاسبات ابری
۲۲	مقدمه:
۲۲	تعریف محاسبات ابری
۲۳	ویژگی ها و خصیصات محاسبات ابری
۲۴	رایانش ابری
۲۶	معماری لایه ای رایانش ابری
۲۶	نرم افزار به عنوان سرویس (اس ای ای)
۲۷	زیر ساخت به عنوان سرویس (آی ای ای اس)
۲۷	بازیگران معماری محاسبات ابری
۲۸	مجازی سازی در رایانش ابری
۲۹	بررسی انواع مختلف توده های ابر، کاربرد ها، مزایا و معایب
۳۰	مدل های زیر ساخت رایانش ابری
۳۱	ابره های عمومی
۳۲	ابره های خصوصی
۳۲	ابره های ترکیبی
۳۳	ابر انجمتی
۳۴	مزایای محاسبات ابری
۳۴	هزینه کمتر
۳۴	اوتتقای نرم افزاری سریع و دائم
۳۴	ظرفیت نامحدود ذخیره سازی
۳۴	قابلیت اطمینان بیشتر به داده ها

۳۵	دسترسی جهانی به اسناد و مقیاس پذیری
۳۵	همکاری گروهی ساده تر
۳۵	مستقل از سخت افزار
۳۶	اصطلاحات و اصول امنیت
۳۶	امنیت
۳۶	امنیت داده ها
۳۶	امنیت اطلاعات
۳۷	کنترل دسترسی
۳۷	مستعد - ملات سایبر
۳۸	امنیت در توده های ابر:
۴۰	نگرانی های امنیتی در محاسبات ابری
۴۳	فواید امنیت برای رایانش ابری
۴۳	امنیت و مقیاس پذیری:
۴۴	امنیت به عنوان یک عامل تمایز در بازار
۴۴	استاندارد کردن واسط ها برای خدمات امنیتی مدیریت شده
۴۴	مقیاس کردن سریع و هوشمند منابع
۴۵	حسابرسی و جمع آوری شواهد:
۴۵	بروز رسانی های دقیق تر، موثرتر و بهینه تر به همراه پیش فرض های
۴۶	حسابرسی و توافقتنامه های سطح سرویس
۴۶	فواید تمرکز منابع
۴۶	پرونده تشخیص ریسک
۴۷	کنترل امنیت اطلاعات
۴۷	مجازی سازی
۵۱	تعریف ابر ناظر
۵۲	تعریف Xen
۵۲	تکنولوژی های مجازی سازی

۵۲	مجازی سازی جزئی
۵۳	مجازی سازی به کمک سخت افزار
۵۳	حامل ها
۵۴	مجازی سازی رومیزی میزبان - مهمان ^۲
۵۵	زیر ساخت مجازی سازی رایانه های رومیزی
۵۵	مجازی سازی سخت افزاری
۵۵	محرمانگی
۵۶	یکپارچه شدن
۵۶	کنترل دستی
۵۷	احراز هویت
۵۷	اس اس ال
۵۹	آی دی باز
۶۰	رمزنگاری
۶۳	اصل کر کهف
۶۳	روشهای رمز نگاری
۶۳	متد های رمز نگاری :
۶۴	رمز نگاری به صورت جریانی
۶۵	رمز نگاری به صورت بلاکی
۶۷	رمزنگاری پیام
۶۷	رمز گشایی پیام
۶۸	معماری شبکه ای محاسبات ابری
۶۹	سیستم رمز نگاری کوله پشتی مرکب هلمن
۶۹	تعریف :
۷۰	تولید کلید
۷۲	فصل سوم: دیگر تحقیقات صورت گرفته
۷۴	مقایسه روشهای کنترل امنیت داده ها
۷۸	مقایسه روش های احراز هویت

۸۰	مقایسه روش های بررسی تمامیت داده های ذخیره شده
۸۳	فصل چهارم: الگوریتم پیشنهادی، ارزیابی و جمع بندی
۸۴	مقدمه
۸۴	رمز گشایی
۸۵	روش ریاضی
۸۶	محرمانگی معادل سیمی
۸۶	۴-۳-اس ای ای ۱
۸۷	تابع در ه سازی اس ای ای ۱
۸۸	کاربردها
۸۸	صحت داده
۸۸	آنالیز و ارزیابی رمز سازی
۹۳	ام دی فایو
۹۶	اضافه کردن بیت های نرم کت
۹۶	افزایش طول
۹۶	تعیین بافر برای MD
۹۷	پردازش پیام در بلاک های ۱۶ کلمه ای
۹۹	خروجی
۹۹	شبیه کد الگوریتم ام دی فایو
۱۰۰	مقایسه ام دی فور و ام دی فایو
۱۰۰	پیاده سازی
۱۰۱	شبیه ساز کلود سیم
۱۰۵	تخمین زمان اجرای برنامه ها
۱۰۷	۴-۱۰-اساس کار تحلیل ایستای بیشترین زمان اجرای برنامه
۱۰۸	تحلیل جریان
۱۰۸	تحلیل سطح پایین
۱۰۹	محاسبات
۱۰۹	معیارهای لازم برای ساختار پیشنهادی

۱۱۰		ساختارهای موثر در تحلیل سطح بالا
۱۱۰		مشخص نمودن حد تکرار حلقه و فراخوانی بازگشتی
۱۱۱		ساختارهای موثر در تحلیل سطح پایین
۱۱۲		کش :
۱۱۳		شیوه ارزیابی
۱۱۳		ملاحظات
۱۱۴		موجودیت های محیط شبیه سازی :
۱۱۴		سناریوی آزمایشات شبیه سازی
۱۱۵		کلام آخر
۱۱۷		منابع

پیشگفتار

سیستم های محاسباتی به طور گسترده ای در حال کامل شدن هستند تا بتوانند پاسخگوی نیازهای بشر در مسائل و کاربردهای مختلف علمی، تجاری، اجتماعی و غیره باشند. این تکامل در ابعاد مختلفی صورت گرفته است. اما در خصوص شناخت صحیح این سیستم محاسباتی به عنوان یک فناوری جدید و جایگاه آن در بین دیگر فناوری های محاسباتی ابهامات زیادی وجود دارد. افرادی که در زمینه رایانش ابری فعالیت دارند، به دلیل اینکه از حوزه های مختلف نظیر نرم افزار، پایگاه داده، شبکه و غیره وارد آن شده اند، دارای دیدگاههای مختلفی در مورد آن هستند که همین موضوع سبب ایجاد تعاریف و رویکردهای مختلف در مورد رایانش ابری شده است. به همین دلیل افرادی که مطالعه در این زمینه را آغاز میکنند، در عمل رتی که چندین منبع یا مقاله مختلف را مطالعه کنند با ابهامات و تعاریف مختلفی مواجه میشوند که ممکن است در بسیاری از موارد این تعاریف قابل جمع شدن با یکدیگر نباشد. خصوصاً در زمانی که لایه های مختلف رایانش ابری مورد بررسی قرار می گیرد. برقراری ارتباط بین تعاریفی که از این لایه ها می شود با همدیگر بسیار چالش برانگیز خواهد بود. از طرفی نگرانی در مورد امنیت داده ها و حفاظت از افشای اطلاعات به سیستم ها و اشخاص بیرون سازمان، تمامی انواع سرویس های محاسبات ابری نگران کننده است و نیازمند به کارگیری اصول ایمنی برای برطرف کردن نگرانی های کاربران می باشد. در این اثر ما به بررسی راهکارهای موجود برای امنیت اطلاعات و انتقال داده در پی ای ای اس^۱ و همچنین معرفی سیاست های مختلف امنیتی در این سطح و ارائه راهکارهای موجود در سیستم های توزیع شده جهت انتقال امن داده و استفاده از شگرد الگوریتم رمزنگاری ام دی فایو^۲ می پردازیم.