

سرشناسه	:	اژدرپور، ساسان، ۱۳۶۶ -
عنوان و نام پدیدآور	:	امنیت داده در محاسبات ابری = Data security in cloud computing / مولف ساسان اژدرپور.
مشخصات نشر	:	تهران: سنجش و دانش، ۱۳۹۶.
مشخصات ظاهری	:	۱۳۷ ص.: مصور (بخشی رنگی)، جدول، نمودار (رنگی).
شابک	:	۱۸۰۰۰۰ ریال: ۹۷۸-۶۰۰-۲۳۲-۹۵۹-۲
وضعیت فهرست نویسی	:	فیا
یادداشت	:	واژنامه.
یادداشت	:	کتابنامه: ص. ۱۳۷.
موضوع	:	محاسبات ابری -- تدابیر ایمنی
موضوع	:	Cloud computing-- Security measures
موضوع	:	محاسبات ابری
موضوع	:	Cloud computing
رده بندی کنگره	:	۱۳۹۶۵۸۵/۷۶۵۸ الف ۴ الف /
رده بندی دیویی	:	۶۷۸۲/۰
شماره کتابشناسی ملی	:	۴۶۶۳۱۵

امنیت داده در محاسبات ابری Data Security In Cloud Computing

مولف:	ساسان اژدرپور
ناشر:	انتشارات سنجش و دانش
تیراژ:	۱۰۰۰ نسخه
توبت چاپ:	اول، ۱۳۹۵
شابک:	۹۷۸-۶۰۰-۲۳۲-۹۵۹-۲
قیمت:	۱۸۰۰۰ تومان

آدرس: خ دانشگاه - تقاطع روانمهر - ساختمان سنجش و دانش پ ۱۲۶

کلیه حقوق مادی و معنوی این اثر محفوظ می باشد.

محاسبات ابری، بعنوان یکی از مهمترین موضوعات در زمینه تکنولوژی اطلاعات معرفی شده است و مزایای فراوانی از جمله کاهش هزینه و سهولت در استفاده دارد اما، به دلیل اینکه در فضای مجازی اینترنت ارائه می شود و اینترنت مکانی نیست که بتوان کنترل کاملی بر روی آن داشت با مسائل بحرانی بسیاری روبرو است که مهمترین آنها امنیت می باشد.

نگرانی در مورد امنیت داده ها، اصلی ترین مانع توسعه محاسبات ابری می باشد. امنیت داده ها عمل محافظت داده ها از انحراف و دستیابی غیرمجاز است. برقراری امنیت داده ها در سطح قابل قبول، نیازمند توجه به اصول امنیت داده ها می باشد. مهمترین این اصول محرمانگی و تمامیت است. محرمانگی حفاظت از افشای اطلاعات به سهیم ها و اشخاص غیرمجاز و تمامیت تضمین اعتبار و درستی اطلاعات است. مسائل امنیت داده ها، بطور بالقوه در تمامی انواع سرویس های محاسبات ابری، نگران کننده است و نیازمند بکارگیری اصول امنیت و مکانیزم های تکنیکی امنیت برای برطرف کردن نگرانی های کاربران می باشد. تاکنون روش های مختلفی برای کنترل امنیت محاسبات ابری ارائه شده است اما همچنان امنیت داده ها گلوگاه محاسبات ابری محسوب می شود.

در این کتاب، با ترکیب تکنیک های احراز هویت بررسی تمامیت داده ها، روشی برای بهبود امنیت داده ها در محاسبات ابری ارائه شده است. مهمترین بررسی های روش پیشنهادی، حفظ اصول امنیت داده ها، قابلیت حسابرسی عمومی و پشتیبانی از عملیات پویایی داده ها می باشند. روش پیشنهادی با استفاده از شبیه ساز CloudSim پیاده سازی شده است. آنالیز مقادیر شاخص های ارزیابی استخراج شده از نتایج آزمایشات شبیه سازی به خوبی نشان می دهد که از یک طرف، فرآیند احراز هویت در روش پیشنهادی در مقایسه با پروتکل تصدیق SSL، هزینه ارتباطی و محاسباتی کمتری به خصوص در سمت سرویس گیرنده دارد و از طرف دیگر، فرآیند بررسی تمامیت با داشتن کمترین هزینه ارتباطی در مقایسه با سایر طرح ها، مصرف پهنای باند شبکه را به حداقل می رساند.

فهرست مطالب

صفحه

عنوان

فصل اول : مقدمه‌ای بر محاسبات ابری

۱۱	۱-۱ مقدمه
۱۲	۱-۲ محاسبات ابری
۱۲	۱-۲-۱ ویژگی‌های کلیدی
۱۴	۱-۲-۲ مدل سرویس
۱۷	۱-۲-۳ مدل‌های پیاده‌سازی
۱۷	۱-۲-۴ تفاوت‌ها و شباهت‌ها با سایر سیستم‌های محاسباتی
۱۹	۱-۲-۵ مزایای محاسبات ابری
۲۱	۱-۳ مشکلات موجود در محاسبات ابری
۲۲	۱-۴ نگرانی‌های امنیتی در محاسبات ابری
۲۶	۱-۵ خلاصه فصل

فصل دوم : امنیت داده‌ها در محاسبات ابری

۲۹	۲-۱ اصول امنیت داده‌ها
۲۹	۲-۱-۱ محرمانگی
۲۹	۲-۱-۲ تمامیت
۲۹	۲-۱-۳ دسترس‌پذیری
۳۰	۲-۲ بررسی روش‌های کنترل امنیت در محاسبات ابری
۳۰	۲-۲-۱ روش ریاضی حفظ امنیت داده‌های محاسبات ابری CYDSM
۳۳	۲-۲-۲ روش ترکیب SACS با معماری محاسبات ابری

۳۶	۲-۲-۳ روش کنترل امنیت بر اساس جداسازی امنیت در لایه‌های متفاوت
۳۸	۲-۲-۴ روش کنترل امنیت PDSM
۴۰	۲-۲-۵ مقایسه روشهای کنترل امنیت
۴۲	۲-۳ بررسی روش‌های احراز هویت در محاسبات ابری
۴۲	۲-۳-۱ استفاده از هویت منته شده و HIBC در تقویت امنیت
۴۳	استفاده از رمزنگاری مبتنی بر هویت سلسله مراتبی HIBC
۴۵	۲-۳-۲ احراز هویت با استفاده از SAP
۴۸	۲-۳-۳ مقایسه روش‌های احراز هویت
۴۹	۲-۴ بررسی روش‌های تأیید تمامیت داده‌های ذخیره شده در محاسبات ابری
۵۰	۲-۴-۱ روش اثبات مالکیت داده‌ها PDP
۵۳	۲-۴-۲ طرح اثبات پربایر، یکیت داده‌ها (DPDP)
۵۸	۲-۴-۳ طرح اثبات‌های قابلیت بازاریابی POP
۵۹	۲-۴-۴ مقایسه روشهای بررسی امنیت داده‌های ذخیره شده
۶۰	۲-۵ خلاصه فصل

فصل سوم: روش پیشنهادی بهبود امنیت داده‌ها

۶۳	۳-۱ مقدمات ساختار پیشنهادی
۶۳	۳-۱-۱ رمزنگاری RSA
۶۴	۳-۱-۲ معماری شبکه‌ای محاسبات ابری
۶۵	۳-۱-۳ درخت درهم سازی مرکب
۶۶	۳-۲ تعاریف
۶۶	۳-۲-۱ رمزگذاری مبتنی بر هویت برای HACC
۶۷	۳-۲-۲ امضای مبتنی بر هویت HACC
۶۷	۳-۲-۳ الگوریتم‌های استفاده شده در DICP
۶۸	۳-۳ ساختار روش پیشنهادی امنیت داده‌ها
۷۰	۳-۴ فاز اول

۷۱	۳-۴-۱ سازماندهی مراکز داده و کاربران در HACCC
۷۳	۳-۵ فاز دوم
۷۴	۳-۵-۱ روش احراز هویت در محاسبات ابری
۷۶	۳-۶ فاز سوم
۷۷	۳-۶-۱ ذخیره سازی داده ها در مراکز داده
۷۸	۳-۶-۲ بررسی تمامیت داده های ذخیره شده
۷۹	۳-۶-۳ عملیات داده های پویا با تضمین تمامیت
۸۴	۳-۷ ارزیابی روش پیشنهادی
۸۴	۳-۷-۱ فرایند احراز هویت با استفاده از APCC
۸۵	۳-۷-۲ فرایند بررسی تمامیت داده ها با DICP
۸۶	۳-۸ ویژگی های روش پیشنهادی
۸۶	۳-۸-۱ حفظ اصول امنیت داده ها
۸۸	۳-۸-۲ استفاده از برجسب های قابل تبدیل Homomorph یا HVTs
۸۸	۳-۸-۳ قابلیت پشتیبانی از عملیات پویایی داده ها
۸۹	۳-۹ شبیه سازی روش پیشنهادی
۹۰	۳-۱۰ خلاصه فصل

فصل چهارم: ارزیابی روش پیشنهادی بهبود امنیت داده ها

۹۳	۴-۱ شبیه ی ارزیابی روش پیشنهادی
۹۳	۴-۱-۱ ملاحظات صورت گرفته در شبیه سازی
۹۳	۴-۱-۲ سناریوی آزمایشات شبیه سازی
۹۵	۴-۱-۳ شاخص های ارزیابی
۹۶	۴-۲ ارزیابی طرح احراز هویت در محاسبات ابری APCC
۹۶	۴-۲-۱ آنالیز کارایی طرح های احراز هویت
۹۸	۴-۲-۲ تجزیه و تحلیل نتایج شبیه سازی طرح های احراز هویت

۴-۳	ارزیابی طرح بررسی تمامیت داده‌ها DICP	۱۰۱
۴-۳-۱	آنالیز کارایی طرح‌های بررسی تمامیت داده‌ها	۱۰۲
۴-۳-۲	تجزیه و تحلیل نتایج شبیه‌سازی طرح‌های بررسی تمامیت داده‌ها	۱۰۴
۴-۴	خلاصه فصل	۱۰۸

فصل پنجم : معرفی شبیه‌ساز CloudSim

۵-۱	شبیه‌ساز CloudSim	۱۱۱
۵-۲	معماری CloudSim	۱۱۲
۵-۳	کلاس‌های موجود در CloudSim	۱۱۳
۵-۴	چارچوب شبیه‌سازی CloudSim	۱۱۷
۵-۵	ارتباط بین موجودات در CloudSim	۱۱۹
۵-۶	استفاده از CloudSim در Netbeans	۱۲۰
۵-۷	خلاصه فصل	۱۲۷
	واژه‌نامه فارسی به انگلیسی	۱۲۶
	فهرست منابع	۱۳۰