

۱۸۴۱۵۲۱
مجله

امنیت رایانش ابری

www.ketab.ir

مؤلفان:

حسین قرائی گرکانی

(هیأت علمی پژوهشگاه ارتباطات و فناوری اطلاعات)

فریبا غفاری

سرشناسه	: قرائی گرکانی، حسین، ۱۳۵۴ -
عنوان و نام پدیدآور	: امنیت رایانش ابری / حسین قرائی گرکانی، فریبا غفاری.
مشخصات نشر	: تهران: برتراندیشان، ۱۳۹۶.
مشخصات ظاهری	: ۳۰۶ ص: مصور (بخشی رنگی)، جدول (بخشی رنگی)، نمودار (بخشی رنگی).
شابک	: ۲۵۰۰۰۰ ریال: ۹-۲۸-۸۸۳۸-۶۰۰-۹۷۸
وضعیت فهرست نویسی	: فیبا
موضوع	: محاسبات ابری
موضوع	: Cloud computing
شناسه افزوده	: غفاری، فریبا. ۱۳۷۰ -
رده بندی کنگره	: ۸۱۳۹۶ الف ۷۶ / ۱۱۱۱۱۱۱۱
رده بندی دیویی	: ۰۶/۷۸
شماره کتابشناسی ملی	: ۴۸۷۲۳۹۵

امنیت رایانش ابری

- مؤلفان: مسین قرائی گرکانی، فریبا غفاری.
- انتشارات: برتراندیشان
- صفحه آراء: اصغر جوزی پور
- طراح جلد: سعید مجازی
- شابک: ۹-۲۸-۸۸۳۸-۶۰۰-۹۷۸
- قیمت: ۲۵۰۰۰۰ ریال
- تیراژ: ۱۰۰۰ نسخه
- نوبت چاپ: اول، ۱۳۹۶



مرکز بخش:

میدان انقلاب، خیابان کارگر شمالی،
خیابان فرصت شیرازی، پلاک ۱۸ واحد ۲
تلفن: ۶۶۵۶۸۱۵۸-۶۶۵۷۵۶۸۱

فهرست مطالب

عنوان	صفحه
مقدمه.....	۱۷
فصل ۱. معرفی رایانش ابری	
۱-۱ مقدمه.....	۱۵
۲-۱ تاریخچه رایانش ابری.....	۱۶
۳-۱ سیستم‌های توزیع شده و رایانش ابری.....	۱۷
۴-۱ تعریف رایانش ابری.....	۱۸
۵-۱ مشخصات ضروری رایانش ابری.....	۲۰
۱-۵-۱ سرور مجزای تقاضا.....	۲۰
۲-۵-۱ خدمات اندازه گیری.....	۲۱
۳-۵-۱ قابلیت کشش.....	۲۱
۴-۵-۱ دسترسی گسترده به شبکه.....	۲۱
۵-۵-۱ به اشتراک گذاری منابع.....	۲۱
۶-۱ مدل‌های سرویس رایانش ابری.....	۲۲
۱-۶-۱ نرم افزار به عنوان سرویس.....	۲۲
۲-۶-۱ سکو به عنوان سرویس.....	۲۲
۳-۶-۱ زیرساخت به عنوان سرویس.....	۲۲
۷-۱ مدل‌های پیاده سازی رایانش ابری.....	۲۳
۱-۷-۱ ابر خصوصی.....	۲۳
۲-۷-۱ ابر اجتماعی.....	۲۴
۳-۷-۱ ابر عمومی.....	۲۴
۴-۷-۱ ابر ترکیبی.....	۲۴
۸-۱ مزایای استفاده از رایانش ابری.....	۲۵
۹-۱ مشکلات موجود در رایانش ابری.....	۲۵
۱-۹-۱ دسترسی پذیری.....	۲۶
۲-۹-۱ نگهداری داده.....	۲۶
۳-۹-۱ چند مستاجری.....	۲۶
۴-۹-۱ کارایی.....	۲۷
۵-۹-۱ منجمد سازی داده.....	۲۷

۶-۹-۱	دستورسی مدیریتی	۲۷
۱۰-۱	امنیت رایانش ابری	۲۸
۱۱-۱	چالش‌های امنیتی در رایانش ابری	۲۹
۱-۱۱-۱	حریم شخصی و محرمانگی	۲۹
۲-۱۱-۱	نگرانی در مورد مالکیت و محل داده‌ها	۳۰
۳-۱۱-۱	وابستگی به سرویس‌های شبکه	۳۱
۴-۱۱-۱	خنده دار شدن صحت داده‌ها	۳۱
۵-۱۱-۱	نگرانی دست‌سی ناخواسته به اطلاعات	۳۲
۶-۱۱-۱	ترک ب ناخواسته داده‌های مشتریان	۳۲
۷-۱۱-۱	فعالیت‌های غیرقانونی در ابر	۳۲
۸-۱۱-۱	عدم شفافیت ابر	۳۲
۹-۱۱-۱	خطرهای آسیب‌پذیری و پیش‌بینی نشده	۳۳
۱۰-۱۱-۱	آسیب‌پذیری‌های مجاز، پسای	۳۳
۱۲-۱	مراجع	۳۳

فصل ۲. سیر تکامل رایانش ابری

۱-۲	مقدمه	۳۵
۲-۲	سیر تکامل سخت‌افزار	۳۶
۱-۲-۲	کامپیوترهای نسل اول	۳۷
۲-۲-۲	کامپیوترهای نسل دوم	۳۹
۳-۲-۲	کامپیوترهای نسل سوم	۴۰
۴-۲-۲	نسل چهارم کامپیوترها	۴۰
۳-۲	سیر تکامل اینترنت	۴۱
۴-۲	دسته‌بندی ابر	۴۴
۵-۲	خلاصه فصل	۴۷
۶-۲	مراجع	۴۸

فصل ۳. مسائل امنیتی رایانش ابری

۱-۳	مقدمه	۴۹
۲-۳	مفاهیم اساسی در امنیت رایانش ابری	۵۰
۱-۲-۳	مجازی‌سازی	۵۰
۲-۲-۳	چند مستأجری	۵۱

۵۲.....	نرم افزار ابر	۳-۲-۳
۵۲.....	برون سپاری داده	۴-۲-۳
۵۲.....	امنیت ذخیره سازی و استاندارد سازی	۵-۲-۳
۵۳.....	اعتماد	۶-۲-۳
۵۳.....	امنیت مدل پیاده سازی و تحویل خدمات	۳-۳
۵۵.....	احراز اصالت	۱-۳-۳
۵۵.....	مجوزدهی	۲-۳-۳
۵۵.....	محرمانگی	۳-۳-۳
۵۶.....	صحت	۴-۳-۳
۵۶.....	انکاب پذیری	۵-۳-۳
۵۶.....	دسترس پذیری	۶-۳-۳
۵۶.....	مسائل امنیتی مجازات	۴-۳
۵۷.....	چندمستاجری	۱-۴-۳
۵۷.....	سکوها و چارچوبها	۲-۴-۳
۵۸.....	واسط کاربری	۳-۴-۳
۵۸.....	کنترل	۴-۴-۳
۵۸.....	مسائل امنیتی محاسباتی و ذخیره سازی	۳-۵
۵۹.....	انتزاع	۱-۵-۳
۶۰.....	صحت	۲-۵-۳
۶۰.....	محرمانگی و حریم خصوصی	۳-۵-۳
۶۱.....	دسترس پذیری	۴-۵-۳
۶۱.....	انحدام	۵-۵-۳
۶۲.....	رمزنگاری	۶-۵-۳
۶۲.....	مسائل امنیتی مجازی سازی	۶-۳
۶۳.....	مدیریت تصاویر	۱-۶-۳
۶۳.....	نظارت بر ماشین های مجازی	۲-۶-۳
۶۴.....	شبکه	۳-۶-۳
۶۴.....	صحت، محرمانگی و حریم خصوصی	۴-۶-۳
۶۵.....	دسترس پذیری	۵-۶-۳
۶۵.....	مسائل امنیتی منابع شبکه، وب و سخت افزار	۷-۳
۶۵.....	استانداردها و پروتکل های ارتباطی	۱-۷-۳

۶۶	جامعیت، محرمانگی و حریم خصوصی	۲-۷-۳
۶۶	حساب‌دهی	۳-۷-۳
۶۶	مسائل امنیتی دسترسی	۸-۳
۶۷	متمرکزسازی داده	۱-۸-۳
۶۷	گواهینامه‌ها	۲-۸-۳
۶۸	احراز اصالت	۳-۸-۳
۶۹	مجوزدهی	۴-۸-۳
۶۹	گمنام‌ری	۵-۸-۳
۶۹	مدل امنیتی اعتماد	۹-۳
۷۰	مراجع	۱۰-۳

فصل ۴. تهدیدات محیط رایانش ابری

۷۱	مقدمه	۱-۴
۷۲	افشای اطلاعات	۲-۴
۷۳	مدیریت نامناسب هویت، گواهینامه‌رسانی	۳-۴
۷۳	واسط‌ها و واسط‌های برنامه‌نویسی نامناسب کاربردی ناامن	۴-۴
۷۴	آسیب‌پذیری‌های سیستم	۵-۴
۷۵	سرقت حساب کاربری	۶-۴
۷۵	کارمندان داخلی مخرب	۷-۴
۷۶	تهدیدات پیشرفته مانا	۸-۴
۷۶	از دست دادن یا دستکاری داده	۹-۴
۷۷	مهاجرت ناآگاهانه به ابر	۱۰-۴
۷۷	سوءاستفاده از خدمات ابر	۱۱-۴
۷۸	ممانعت از سرویس	۱۲-۴
۷۸	مسائل امنیتی فناوری به‌اشتراک گذاشته‌شده	۴-۱۳
۷۸	محاسبات غیرقابل اعتماد در سرورهای راه دور	۱۴-۴

فصل ۵. آسیب‌پذیری‌های موجود در محیط‌های رایانش ابری

۸۱	مقدمه	۱-۵
۸۲	آسیب‌پذیری‌های فناوری هسته	۲-۵
۸۲	فرار ماشین مجازی	۱-۲-۵
۸۲	تسلط بر نشست و سرقت	۲-۲-۵

۸۳.....	۳-۲-۵ رمزنگاری‌های نامناسب و ضعیف
۸۳.....	۲-۵ آسیب‌پذیری‌های مشخصه‌های اصلی ابر
۸۳.....	۱-۳-۵ دسترسی بدون احراز اصالت به واسط مدیریت
۸۳.....	۲-۳-۵ آسیب‌پذیری‌های پروتکل‌های اینترنت
۸۴.....	۳-۳-۵ آسیب‌پذیری‌های بازیابی داده‌ها
۸۴.....	۴-۳-۵ طفره رفتن از پرداخت صورت حساب
۸۴.....	۴-۵ نقص در کنترل‌های امنیتی شناخته شده
۸۴.....	۱-۴-۵ کنترل‌های نامناسب در شبکه
۸۵.....	۲-۴-۵ فرایند مدیریت ضعیف کلید
۸۵.....	۳-۴-۵ عدم رفق‌پذیری معیارهای امنیتی در زیرساخت ابر
۸۵.....	۵-۵ آسیب‌پذیری‌های مؤلفه‌های معماری ابر
۸۷.....	۱-۵-۵ آسیب‌پذیری‌های خطای ساخت نرم افزار ابر
۹۲.....	۲-۵-۵ امکانات نظارت و واکنش‌های نامناسب
۹۲.....	۶-۵ آسیب‌پذیری‌های معرفی شده توسط ENISA
۹۲.....	۱-۶-۵ آسیب‌پذیری‌های AAA
۹۳.....	۲-۶-۵ آسیب‌پذیری‌های فوق ناظر
۹۳.....	۳-۶-۵ نقص در ایزوله سازی منابع
۹۴.....	۴-۶-۵ رمزگذاری ضعیف و عدم رمزنگاری داده‌ها در هنگام آرشیوها یا انتقال داده
۹۴.....	۵-۶-۵ فرایند مدیریت کلید ضعیف
۹۵.....	۶-۶-۵ آنترابی پائین برای تولید اعداد تصادفی
۹۵.....	۷-۶-۵ فقدان راه حل ها و فناوری ها استاندارد
۹۵.....	۸-۶-۵ عدم امکان جرم‌یابی
۹۶.....	۷-۵ مراجع
	فصل ۶. مخاطرات رایانش ابری
۹۷.....	۱-۶ مقدمه
۹۸.....	۲-۶ دارایی‌های رایانش ابری
۱۰۰.....	۳-۶ مخاطرات مشترک در ابرهای خصوصی و عمومی
۱۰۱.....	۱-۳-۶ بررسی مخاطرات سازمانی و سیاست
۱۰۸.....	۲-۳-۶ مخاطرات فنی و عملیاتی
۱۱۹.....	۳-۳-۶ مخاطرات قانونی
۱۲۲.....	۴-۳-۶ ده مخاطره برتر OWASP

۴-۶	مراجع	۱۲۹
فصل ۷. حملات موجود در محیط‌های رایانش ابری		
۱-۷	مقدمه	۱۳۱
۲-۷	حملات جلوگیری از سرویس	۱۳۱
۳-۷	حملات تزریق بدافزار در ابر	۱۳۲
۴-۷	حملات احراز اصالت	۱۳۲
۵-۷	حملات مرد میانی	۱۳۳
۶-۷	حملات داخلی	۱۳۳
۷-۷	حملات سرریزی بافر	۱۳۴
۸-۷	حملات کاربر بدنام	۱۳۴
۹-۷	اسکن کردن پورت	۱۳۴
۱۰-۷	حملات بر روی مجازات‌های	۱۳۵
۱۱-۷	حملات کانال درپشتی	۱۳۵
۱۲-۷	حمله‌ی بسته‌بندی امضای XML	۱۳۵
۱۳-۷	حملات مهندسی اجتماعی	۱۳۶
۱۴-۷	حملات Guest Hopping	۱۳۶
۱۵-۷	حملات تزریق SQL	۱۳۷
۱۶-۷	حملات کانال جانبی	۱۳۷
۱۷-۷	حملات XSS	۱۳۸
۱۸-۷	حملات مکان مشترک	۱۳۸
۱۹-۷	فرار ماشین مجازی	۱۳۸
۲۰-۷	حملات حذف رکوردهای تکراری	۱۳۹
۲۱-۷	مراجع	۱۴۰
فصل ۸. استانداردهای رایج در رایانش ابری		
۱-۸	مقدمه	۱۴۱
۲-۸	استانداردهای رایج در امنیت رایانش ابری	۱۴۱
۱-۲-۸	احراز اصالت و اختیاری	۱۴۲
۲-۲-۸	محرمانگی	۱۴۳
۳-۲-۸	جامعیت	۱۴۴
۴-۲-۸	مدیریت هویت	۱۴۵

۵-۲-۸	نظارت امنیت و پاسخ به حوادث	۱۴۵
۶-۲-۸	کنترل‌های امنیتی	۱۴۶
۷-۲-۸	مدیریت سیاست امنیتی	۱۴۷
۸-۲-۸	دسترس پذیری	۱۴۸
۳-۸	استانداردهای رایج برای تعامل پذیری و قابلیت انتقال در رایانش ابری	۱۴۹
۴-۸	استانداردهای رایج کارایی در رایانش ابری	۱۵۰
۵-۸	استانداردهای رایج در زمینه قابلیت دسترس پذیری در رایانش ابری	۱۵۲
۶-۸	مراجع	۱۵۲

فصل ۹. کنترل‌های امنیتی در رایانش ابری

۱-۹	مقدمه	۱۵۳
۲-۹	مدل سرویس ابر و تقسیم وظایف امنیتی	۱۵۳
۳-۹	مدل‌های پیاده‌سازی ابر	۱۵۷
۱-۳-۹	امنیت در مدل‌های ابر	۱۵۸
۲-۳-۹	مسائل امنیتی در ابر عمومی	۱۵۹
۳-۳-۹	مسائل امنیتی در ابر خصوصی	۱۵۹
۴-۳-۹	مسائل امنیتی در ابر ترکیبی	۱۶۰
۴-۹	عوامل‌های ابر	۱۶۰
۱-۴-۹	مستأجر ابر	۱۶۱
۲-۴-۹	ارائه‌کننده ابر	۱۶۱
۵-۹	نگاشت استانداردها در مدل ابر	۱۶۱
۶-۹	ماتریس کنترلی ابر ارائه‌شده توسط CSA	۱۶۲
۱-۶-۹	امنیت واسط و برنامه کاربردی	۱۶۹
۲-۶-۹	تطابق و اطمینان ممیزی	۱۷۴
۳-۶-۹	مدیریت تداوم کسب‌وکار	۱۷۸
۴-۶-۹	کنترل تغییرات و مدیریت بیکربندی	۱۹۱
۵-۶-۹	امنیت داده و مدیریت چرخه حیات اطلاعات	۱۹۶
۶-۶-۹	امنیت مراکز داده	۲۰۰
۷-۶-۹	مدیریت کلید و رمزنگاری	۲۰۴
۸-۶-۹	مدیریت مخاطرات و قانون‌گذاری	۲۰۷
۹-۶-۹	امنیت منابع انسانی	۲۱۷
۱۰-۶-۹	مدیریت دسترسی و شناسایی	۲۲۵

۲۳۵.....	۱۱-۶-۹ زیرساخت و مجازی سازی
۲۴۶.....	۱۲-۶-۹ تعامل پذیری و قابلیت حمل
۲۴۸.....	۱۳-۶-۹ مدیریت حوادث، کشف الکترونیکی و جرم یابی در ابر
۲۵۱.....	۱۴-۶-۹ مدیریت آسیب پذیری و تهدیدات
۲۵۳.....	۷-۹ دامنه های کنترلی ITU-T X.1631
۲۵۷.....	۸-۹ تلفیق استانداردهای امنیتی و معماری امنیتی
۲۵۹.....	۹-۹ مراجع

فصل ۱۰ امنی ری ریفه های ابر

۲۶۱.....	۱-۱۰ مقدمه
۲۶۱.....	۲-۱۰ امن سازی انباره ر ابر
۲۶۲.....	۱-۲-۱۰ روش های رمزنگاری محط
۲۶۲.....	۳-۱۰ امن سازی شبکه
۲۶۴.....	۴-۱۰ امن سازی فوق ناظر
۲۶۵.....	۱-۴-۱۰ جداسازی ترافیک مدیریتی و مانشیر مجار
۲۶۵.....	۲-۴-۱۰ کنترل دسترسی در دسترسی به VLAN
۲۶۶.....	۳-۴-۱۰ امن سازی واسط مدیریتی خارج از محدوده
۲۶۶.....	۴-۴-۱۰ بروزرسانی وصله های امنیتی فوق ناظر
۲۶۶.....	۵-۴-۱۰ مجوزدهی مناسب
۲۶۷.....	۶-۴-۱۰ غیرفعال کردن سرویس های غیر ضروری
۲۶۷.....	۵-۱۰ امن سازی محیط مجازی سازی
۲۶۷.....	۱-۵-۱۰ امنیت سیستم عامل مهمان
۲۶۸.....	۲-۵-۱۰ امنیت زیرساخت مجازی
۲۶۹.....	۶-۱۰ مراجع

فصل ۱۱ پیوست الف - جدول الزامات و کنترل های امنیتی CSA و ITU

فصل ۱۲ اختصارات

فصل ۱۳ فهرست واژگان

امروزه یکی از چالش‌های اصلی سازمان‌ها، بهینه‌سازی استفاده از فناوری است در دهه‌های گذشته بسیاری از سازمان‌ها با مشکلاتی چون هزینه بالای خرید تجهیزات رایانه‌ای، اتلاف منابع رایانه‌ای به دلیل عدم استفاده مناسب، کمبود فضای نگهداری اطلاعات و مباحث مشابه مواجه بودند در این سال‌ها پروفیسور جان مکاری اعلام کرد محاسبات ممکن است روزی به عنوان یک ابزار مفید عمومی سازمان‌دهی شود با بهره‌گیری از این فرضیه، توسعه‌های بسیاری در حوزه سیستم‌های توزیع‌شده، خوشه‌های کامپیوتریو شبکه‌های کامپیوتری انجام شد و در نهایت منجر به معرفی مفهوم رایانش ابری شد رایانش ابری مدلی است که امکان دسترسی فراگیر، آسان و به محض تقاضا توسط شبکه را به منابع محاسباتی قابل پیکربندی مشترک (مانند شبکه‌ها، سرورها، حافظه، برنامه‌های کاربردی و سرویس‌ها فراهم می‌سازد که این منابع می‌تواند به سرعت فراهم شده و با کم‌ترین تلاش مدیریتتیا تعامل با ارائه‌دهنده سرویس، در دسترس قرار گیرد این مدل ابر از پنج مشخصه ضروری شامل سرویس به محض تقاضا، خدمات انعطاف‌پذیری شده، قابلیت کشسانی سریع، دسترسی گسترده به شبکه و به اشتراک‌گذاری منابع، سه مدل سرویس شامل نرم‌افزار به عنوان سرویس، سکو به عنوان سرویس و زیرساخت به عنوان سرویس و چهار مدل پیاده‌سازش شامل، بر خصوصی، عمومی، ترکیبی و ابر اجتماعی تشکیل شده است امروزه شرکت‌هایی مانند آمازون، گوگل، اوراکل و هزاران شرکت توسعه‌یافته دیگر از رایانش ابری استفاده کرده و به عنوان ارائه‌دهندگان اصلی آن شناخته می‌شوند از دید مشتری، تعداد بسیار بالایی از سازمان‌ها و افراد نیز از این محیط برای پردازش، نگهداری داده و یا حتی برنامه‌نویسی استفاده می‌کنند این مساله منجر به اهمیت بسیار بالای امنیت در این محیط می‌شود مطالعات اخیر نشان داده‌اند که مقوله امنیت، بزرگ‌ترین سد پیش روی این فناوری است که گسترش آنرا کند نموده است تهدیدها، امنیتی متنوعی وجود دارد که قادر است اصول امنیتی ابر را مخدوش سازد تعداد زیادی چالش در حوزه امنیت رایانش ابری مطرح می‌گردد که نیاز به مقابله و برطرف‌سازی دارد از این‌رو سازمان‌ها به میزان زیادی در حوزه امنیت این محیط سرمایه‌گذاری کرده و اقدام می‌کنند.

امنیت رایانش ابری در اغلب موارد تفاوتی با کنترل‌های امنیتی موجود در دیگر محیط‌های فناوری اطلاعات ندارد با این حال با توجه به مدل‌های سرویس پیاده‌سازی شده، مدل‌های عملیاتی و فناوری‌های استفاده شده برای برقرار ساختن سرویس‌های ابر، امکان آن هست که رایانش ابری نسبت به دیگر راهکارهای فناوری اطلاعات سنتی مخاطرات مختلفی را به همراه داشته باشد

آغاز نوشتار کتابی که پیش‌روی خوانندگان محترم قرار دارد بر اساس نیازی که به مبحث توسعه رایانش ابری و امنیت آن در معماری شبکه ملی و خدمات امنیتی مرتبط با آن در مرکز تحقیقات مخابرات ایران برمی‌گردد شبکه ملی اطلاعات کشور، شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیرب‌ها و مراکز داده است به صورتی که درخواست‌های دسترسی داخلی و اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به

هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترنت، خصوصی و امن داخلی در آن فراهم شود.

یکی از ارکان مهم و خدمات اصلی شبکه ملی در کشور، راه‌اندازی و توسعه رایانش ابری در سطوح مختلف شبکه ملی و به طور اخص در مراکز داده می‌باشد این خدمات با هدف کاهش هزینه، بهینه‌سازی اتلاف منابع و توسعه زیرساخت فناوری در کشور انجام می‌شود راه‌اندازی رایانش ابری، ملزم به شناسایی امنیت این فضا و به‌سازی آن است کنترل‌های امنیتی ابر در یک‌جا چند لایه پیاده‌سازی می‌شوند مسئولیت‌های فراهم‌کننده و مصرف‌کننده برای برقراری امنیت در مدل‌های مختلف سرویس ابر کاملاً متفاوت است. از این رو در این کتاب در نظر داریم به شناسایی رایانش ابری، امنیت رایانش ابری، استانداردها و الزامات رایانش ابری و راهکارهای امن‌سازی این محله می‌پردازیم.

www.ketab.ir