

ایجاد زیرساخت برای امنیت ابری راه کارها

تالیف

راگو یلوری

انریکه کاسترو-لئون

ترجمه

دکتر امید مهدی صادقی

عضو هیئت علمی دانشگاه خوارزمی

مهندس حسین علیمردی

کارشناس مرکز تخصصی آپا خوارزمی



دانشگاه خوارزمی

تهران، ۱۳۹۸

سرشناسه	یلوری، راگو Yeluri, Raghu
عنوان و نام پدیدآور	ایجاد زیرساخت برای امنیت ابری راه کارها/مولفان راگو یلوری، انریکه کاسترو-لئون ؛ مترجمان امیدمهدی عبادتی، حسین علیمراد.
مشخصات نشر	تهران: دانشگاه خوارزمی، ۱۳۹۸.
مشخصات ظاهری	۳۰۹ص:، مصور، جدول شمول دارد.
شابک	۹۷۸-۶۰۰-۸۵۸۷-۲۷-۹
وضعیت فهرست نویسی	فیب
یادداشت	عنوان اصلی: Building the infrastructure for cloud security : a solutions view, 2014.
موضوع	محاسبات ابری -- تدابیر ایمنی
موضوع	Cloud computing-- Security measures
موضوع	رمزگذاری داده‌ها
موضوع	Data encryption (Computer science)
شناسه افزوده	کاسترو-لئون، انریکه
شناسه افزوده	Castro-Leon, Enrique
شناسه افزوده	عبادت، امیدمهدی، ۱۳۶۱- مترجم
شناسه افزوده	مراد، حسین، ۱۳۶۸- مترجم
شناسه افزوده	دانشگاه خوارزمی
رده بندی کنگره	۹۱۳۹۸-۸۵/۸-۸۷۶
رده بندی دیویی	۶۷۸۲/۰۰۴
شماره کتابشناسی ملی	۵۶۲۹۷۰۲



شناسنامه کتاب

عنوان کتاب: ایجاد زیرساخت برای امنیت ابری
تألیف: راگو یلوری- انریکه کاسترو-لئون
ترجمه: امید مهدی عبادتی- حسین علیمراد
ناشر: دانشگاه خوارزمی
چاپ و صحافی: دانشگاه خوارزمی
صفحه آرا: لیلا کشاورز
طراح جلد: لیلا کشاورز
شماره: ۵۰۰ نسخه
قیمت: ۲۴۰۰۰ ریال
شابک: ۹۷۸-۶۰۰-۸۵۸۷-۲۷-۹

نشانی: خ دکتر مفتاح، شماره ۴۳، کدپستی ۳۷۵۵۱-۳۱۹۷۹، تلفن مرکز پخش: ۸۸۳۱۱۸۶۶

pub@khu.ac.ir

www.khu.ac.ir

فهرست مطالب

۱.	فصل اول: مبانی رایانش ابری	۲۱
۱-۱	تعریف ابر	۲۲
۱-۱-۱	مشخصات ضروری ابر	۲۳
۱-۱-۲	مدلهای خدمات ابر	۲۴
۱-۱-۳	مدلهای استفاده از ابر	۲۵
۱-۱-۴	پیشنهاد ارزش ابر	۲۶
۲-۱	چینه تاریخی	۲۸
۱-۲-۱	همان سه بهار سنتی	۲۹
۲-۲-۱	تحول مرکز داده: از طبقات تا شبکه‌های خدمات	۳۱
۳-۲-۱	ابر به عنوان روش جدید برای IT	۳۴
۳-۱	امنیت به عنوان خدمات	۳۶
۱-۳-۱	مرزهای امنیت جدید شرکت	۳۷
۲-۳-۱	نقشه راه برای امنیت در ابر	۴۲
۴-۱	خلاصه	۴۳
۲.	فصل دوم: ابر معتبر، بررسی امنیت و سازگاری	۴۵
۱-۲	ملاحظات ایمنی برای ابر	۴۶
۱-۱-۲	امنیت ابر، اعتماد و اطمینان	۴۸
۲-۱-۲	روندهای تاثیرگذار بر امنیت مرکز داده	۵۰
۳-۱-۲	چالش‌های امنیت و سازگاری	۵۲
۴-۱-۲	ابرهای معتبر	۵۴
۲-۲	زیرساخت رایانش معتبر	۵۶
۳-۲	مدلهای مصرف ابر معتبر	۵۷

۵۹	۱-۳-۲- مدل مصرف یکپارچگی راهاندازی
۶۰	۲-۳-۲- درک ارزش یکپارچگی راهاندازی پلتفرم
۶۱	۳-۳-۲- مدل مصرف راهاندازی ماشین مجازی معتبر
۶۳	۴-۳-۲- مدل مصرف محافظت از داده
۶۴	۵-۳-۲- مدل مصرف یکپارچگی و تأیید اعتبار زمان مصرف
۶۵	۴-۲- پیشنهاد ارزش ابر معتبر برای مستاجران ابر
۶۶	۴-۲- وایای خدمات ابر در زنجیره رایانش معتبر
۶۸	۵-۲- خلاصه
۶۹	۳. فصل سوم: یکپارچگی راهاندازی پلتفرم، مبانی برای منابع رایانش معتبر
۷۰	۱-۳- بلوک‌های سازنده ابرهای معتبر
۷۱	۲-۳- یکپارچگی راهاندازی پلتفرم
۷۱	۳-۳- ریشه‌های اعتماد: RTM، RTR و RTS در مفهوم TXT اینتل
۷۲	۱-۳-۳- فرایند راهاندازی اندازه‌گیری شد
۷۶	۲-۳-۳- تأیید اعتبار
۷۷	۴-۳- منابع رایانش معتبر
۷۹	۱-۴-۳- اصول عملیات TCP
۸۰	۲-۴-۳- ایجاد منبع
۸۰	۳-۴-۳- تعیین جایگاه بارکاری
۸۱	۴-۴-۳- انتقال بارکاری
۸۲	۵-۴-۳- گزارش سازگاری برای خدمات ابر/بارکاری
۸۲	۵-۳- معماری مرجع راهکار برای TCP
۸۳	۱-۵-۳- لایه سخت‌افزار
۸۴	۲-۵-۳- لایه سیستم‌عامل/هایپروایزر

- ۳-۵-۳- لایه مدیریت ابر/مجازی سازی و اعتبارسنجی/تائید اعتبار ۸۵
- ۳-۵-۴- لایه مدیریت امنیت ۸۷
- ۳-۶-۱- اجرای مرجع: مطالعه موردی بورس تایوان ۹۰
- ۳-۶-۱- معماری راهکار برای TWSE ۹۱
- ۳-۶-۲- شروع استفاده از منبع رایانش معتبر ۹۳
- ۳-۶-۳- تائید اعتبار از راه دور با HyTrust ۹۴
- ۳-۶-۴- مثال مورد کاربرد: ایجاد منابع رایانش معتبر و انتقال بارکاری ۹۶
- ۳-۶-۵- اعتماد پلتفرم و امنیت یکپارچه و گسترده با McAfee ePO ۹۷
- ۳-۷- خلاصه ۱۰۲
- ۴- فصل چهارم: تایید اعتماد، اثبات قابلیت اعتماد ۱۰۳
- ۴-۱- تائید اعتبار ۱۰۴
- ۴-۱-۱- معماری سنجش یکپارچگی ۱۰۶
- ۴-۱-۲- معماری سنجش یکپارچگی ناهش رفته سیاست ۱۰۶
- ۴-۱-۳- تائید از راه دور معنایی ۱۰۷
- ۴-۲- فرایند تائید اعتبار ۱۰۷
- ۴-۲-۱- پروتکل تائید از راه دور ۱۰۷
- ۴-۲-۲- جریان سنجش یکپارچگی ۱۱۰
- ۴-۳- اولین اجرای تائید اعتبار تجاری: پلتفرم تائید اعتماد اینتل ۱۱۲
- ۴-۴- پلتفرم Mt. Wilson ۱۱۴
- ۴-۴-۱- معماری Mt. Wilson ۱۱۶
- ۴-۴-۲- فرایند تائید Mt. Wilson ۱۱۸
- ۴-۵- امنیت Mt. Wilson ۱۲۲
- ۴-۶- API های اعتماد تعیین فهرست سفید و مدیریت Mt. Wilson ۱۲۴

۱۲۶	۴-۶-۱- API های Mt. Wilson
۱۲۸	۴-۶-۲- مشخصات درخواست API
۱۲۹	۴-۶-۳- پاسخ API
۱۳۰	۴-۶-۴- کاربرد Mt. Wilson API
۱۳۱	۴-۶-۵- استفاده از Mt. Wilson
۱۳۲	۴-۶-۶- مثال‌های برنامه نویسی Mt. Wilson
۱۳۵	۴-۷- خلاصه
۱۳۷	۵. فصل پنجم: کنترل مرز در ابر، برجسب‌زنی جغرافیایی و برجسب‌زنی دارایی
۱۳۸	۵-۱- موقعیت جغرافیایی
۱۳۹	۵-۲- تعیین محدوده جغرافیایی
۱۴۱	۵-۳- برجسب‌زنی دارایی
۱۴۲	۵-۴- کاربرد منابع رایانش معتبر با برجسب‌زنی جغرافیایی
۱۴۵	۵-۴-۱- مرحله ۱: تأیید پلتفرم و راه‌اندازی پیروایزر امن
۱۴۵	۵-۴-۲- مرحله ۲: انتقال امن مبتنی بر اعتماد
۱۴۵	۵-۴-۳- مرحله ۳: انتقال امن مبتنی بر اعتماد و موقعیت جغرافیایی
۱۴۶	۵-۵- اضافه کردن برجسب‌زنی جغرافیایی به راهکار منابع رایانش معتبر
۱۴۷	۵-۵-۱- لایه سخت‌افزار (سرورها)
۱۴۸	۵-۵-۲- لایه سیستم‌عامل و هایپروایزر
۱۴۸	۵-۵-۳- لایه مجازی‌سازی، مدیریت ابر، و اعتبارسنجی و تأیید
۱۴۹	۵-۵-۴- لایه مدیریت امنیت
۱۵۰	۵-۵-۵- فراهم‌سازی و مدیریت چرخه عمر برای برجسب‌های جغرافیایی
۱۵۱	۵-۶- جریان کاری و چرخه عمر برجسب جغرافیایی
۱۵۱	۵-۶-۱- ایجاد برجسب

۱۵۲.....	۵-۶-۲- تعیین فهرست سفید برچسب ها
۱۵۲.....	۵-۶-۳- فراهم سازی برچسب
۱۵۵.....	۵-۶-۴- تائید و عدم تائید برچسب های دارایی و برچسب های جغرافیایی
۱۵۶.....	۵-۶-۵- تائید برچسب های جغرافیایی
۱۵۶.....	۵-۷-۷- معماری فراهم سازی برچسب جغرافیایی
۱۵۷.....	۵-۷-۱- خدمات فراهم سازی برچسب
۱۵۹.....	۵-۷-۲- عامل فراهم سازی برچسب
۱۶۰.....	۵-۷-۳- خدمات مدیریت برچسب و ابزار مدیریت
۱۶۱.....	۵-۷-۴- خدمات تائید
۱۶۴.....	۵-۸-۱- فرایند فراهم سازی برچسب جغرافیایی
۱۶۴.....	۵-۸-۱- مدل فشاری
۱۶۵.....	۵-۸-۲- مدل کششی
۱۶۸.....	۵-۹-۱- اجرای مرجع
۱۶۸.....	۵-۹-۱- مرحله ۱
۱۶۹.....	۵-۹-۲- مرحله ۲
۱۷۰.....	۵-۹-۳- مرحله ۳
۱۷۱.....	۵-۹-۴- مرحله ۴
۱۷۳.....	۵-۱۰- خلاصه
۱۷۵.....	۶. فصل ششم: امنیت شبکه در ابر
۱۷۶.....	۶-۱- شبکه ابر
۱۷۶.....	۶-۱-۱- اجزای امنیت شبکه
۱۷۸.....	۶-۱-۲- متعادل سازهای بار
۱۷۸.....	۶-۱-۳- دستگاه های تشخیص نفوذ

- ۱۷۸..... ۴-۱-۶- کنترلگرهای تحویل برنامه کاربردی
- ۱۷۹..... ۲-۶- امنیت سرتاسری در ابر
- ۱۸۰..... ۱-۲-۶- امنیت شبکه: امنیت سرتاسری: فایروال ها
- ۱۸۰..... ۲-۲-۶- امنیت شبکه: امنیت سرتاسری: VLAN ها
- ۱۸۱..... ۳-۲-۶- امنیت سرتاسری برای VPN های سایت به سایت
- ۱۸۳..... ۴-۲-۶- امنیت هایپروایزر
- ۱۸۴..... ۲-۶- امنیت مهمان ماشین مجازی
- ۱۸۵..... ۳-۶- امنیت تعریف شده توسط نرم افزار در ابر
- ۱۹۰..... ۱-۳-۶- OpenStack
- ۱۹۱..... ۲-۳-۶- امنیت شبکه OpenStack
- ۱۹۳..... ۳-۳-۶- قابلیت ها و مثال های امنیت شبکه
- ۱۹۶..... ۴-۶- خلاصه
- ۱۹۷..... ۷- فصل هفتم: مدیریت هویت و کنترل برای برها
- ۱۹۹..... ۱-۷- چالش های هویت
- ۲۰۰..... ۱-۱-۷- کاربردهای هویت
- ۲۰۲..... ۲-۱-۷- اصلاح هویت
- ۲۰۲..... ۳-۱-۷- ابطال هویت
- ۲۰۳..... ۲-۷- الزامات سیستم مدیریت هویت
- ۲۰۴..... ۱-۲-۷- ویژگی های کنترل کاربر اصلی
- ۲۰۵..... ۳-۷- الزامات اصلی برای راهکار مدیریت هویت
- ۲۰۵..... ۱-۳-۷- مسئولیت پذیری
- ۲۰۵..... ۲-۳-۷- اعلان
- ۲۰۶..... ۳-۳-۷- بی نامی

۲۰۶	۷-۳-۴- حداقل سازی داده
۲۰۷	۷-۳-۵- امنیت ویژگی
۲۰۷	۷-۳-۶- حریم شخصی ویژگی
۲۰۷	۷-۴- بازنمایی های هویت و مطالعات موردی
۲۰۸	۷-۴-۱- مجوزهای PKI
۲۰۹	۷-۴-۲- بررسی امنیت و حریم شخصی
۲۱۰	۷-۴-۳- اتحاد هویت
۲۱۲	۷-۴-۴- ورود یکپارچه
۲۱۲	۷-۵- فناوری های هویت - امنیت
۲۱۳	۷-۵-۱- پشتیبانی مبتنی بر اتم
۲۱۸	۷-۶- خلاصه
۲۱۹	۸. فصل هشتم: ماشین های مجازی معتبر، تم مین یکپارچگی ماشین های مجازی در ابر
۲۲۰	۸-۱- الزامات ماشین های مجازی معتبر
۲۲۴	۸-۲- تصاویر ماشین مجازی
۲۲۵	۸-۲-۱- قالب مجازی سازی باز (OVF)
۲۲۷	۸-۳- معماری مفهومی برای ماشین های مجازی معتبر
۲۲۸	۸-۳-۱- مشتری Mystery Hill (MH)
۲۲۹	۸-۳-۲- سرور سیاست و مدیریت کلید Mystery Hill (KMS)
۲۲۹	۸-۳-۳- اتصال Mystery Hill
۲۳۱	۸-۳-۴- سرور تأیید اعتماد
۲۳۲	۸-۴- جریان های کاری برای ماشین های مجازی معتبر
۲۳۴	۸-۵- استفاده از ماشین های مجازی معتبر با OpenStack
۲۳۹	۸-۶- خلاصه

۲۴۱	۹. فصل نهم: طراحی مرجع برای انفجار ابر امن
۲۴۲	۹-۱- مدل های کاربرد انفجار ابر
۲۴۲	۹-۱-۱- توضیح انفجار ابر
۲۴۷	۹-۲- مدل های استفاده از مرکز داده
۲۴۸	۹-۲-۱- ابرهای ترکیبی معتبر
۲۵۰	۹-۳- معماری مرجع انفجار ابر
۲۵۱	۹-۳-۱- محیط امن ساخته شده با بهترین فعالیت ها
۲۵۲	۹-۱-۲- مدیریت ابر
۲۵۲	۹-۳-۳- مدیریت دسترسی و هویت ابر
۲۵۳	۹-۳-۴- تفکیک منابع ابر ترایک و داده
۲۵۳	۹-۳-۵- آسیب پذیری و مدیریت بسته
۲۵۳	۹-۳-۶- سازگاری
۲۵۶	۹-۴- ملاحظات و توپولوژی شبکه
۲۶۰	۹-۵- ملاحظات طراحی امنیت
۲۶۰	۹-۵-۱- تقویت های پروایزر
۲۶۰	۹-۵-۲- فایروال ها و تفکیک شبکه
۲۶۳	۹-۵-۳- استفاده از فایروال در شبکه مدیریت
۲۶۴	۹-۵-۴- ایجاد شبکه مجازی
۲۶۴	۹-۵-۵- نرم افزار آنتی ویروس
۲۶۵	۹-۵-۶- امنیت مدیریت ابر
۲۷۳	۹-۶- ملاحظات عملی برای انتقال ماشین مجازی
۲۷۵	۹-۷- خلاصه
۲۷۷	۱۰. فهرست اسامی خاص

در دوران حرفه‌ای کاری خود در حوزه فناوری اطلاعات و ارتباطات، از برنامه‌نویسی که از سال ۱۹۹۱ شروع نموده‌ام تاکنون که بصورت تخصصی طی چندین سال گذشته در حوزه امنیت شبکه و امنیت داده کار می‌نمایم، تحولات بسیار زیادی را دیده‌ام. اما مسایل و مخاطرات امنیتی این حوزه، امروزه با توجه به وابستگی صنایع و سازمانها و تنیده شدن کلیه فرآیندها و کارکردها و همچنین رشد آنها به فناوری اطلاعات، موجب ایجاد نگرانی و ریسک‌های امنیتی شده است. لذا بر این اساس و پس از تصنیف کتاب ارائه چارچوب امنیت شبکه پویا از طریق میکروفايروال‌ها: معماری امن هابری، تصمیم به ترجمه این کتاب معتبر در حوزه امنیت ابری با نگاهی به ارائه راه‌حل‌های مختلف نمودم.

مخاطرات امنیتی حوزه فناوری اطلاعات از نفوذهای مختلف در شرکت‌ها و صنایع بزرگ تا نفوذ به سامانه‌ها و داده‌های سازمانها و شرکت‌ها و از طرفی کارکردها و تنظیمات و اشتباهات مدیران سرور و شبکه هر کدام می‌تواند یک رمان با تجارت پایدار را براحتی دچار تهدیدات و ریسک‌های جبران‌ناپذیر نماید.

امروزه در سازمان‌ها، داده و امنیت آنها، اساسی‌ترین رکن آن سازمان یا شرکت به شمار می‌آیند.

با رویکرد جدید در دنیا و تحولات صورت گرفته از سال ۲۰۰۶ و ارائه سرویس‌های مختلف بر پایه ابر، امروزه بهره‌گیری از آن در غالب محاسبات ابری عمومی، خصوصی یا هیبریدی بر کسی پوشیده نیست. تحولاتی که بر پایه سرویس EC2 آمازون در سال ۲۰۰۶ شروع و توسط مایکروسافت و آی‌بی‌ام در اواخر سال ۲۰۰۸ و ابتدای سال ۲۰۱۱ به تحولات بزرگی دست یافت.

شاید در ابتدا بهره‌گیری از این سرویس‌ها در حد شرکت‌ها و سازمان‌های بزرگ می‌بود، اما امروزه سیر تحول محاسبات ابری در ارائه به کسب و کارهای کوچک مسیری بسیار روشن و بصره‌ای را پدید آورده است. کاهش هزینه‌ها، هزینه‌های مستمر زیرساختی، در دسترس بودن در لحظه سرویس‌ها، شرایط ذخیره‌سازی داده‌ها، مجازی‌سازی، گسترش زیرساختی پویا، اختصاص پهنای باند مناسب، پردازش سریع‌تر و پشتیبانی آنلاین امروزه توانسته است، حتی شرکت‌ها و سازمان‌های با داده‌های حساس را به سمت رایانش ابری بکشاند.

این حوزه نیز همانند بسیاری از حوزه‌های دیگر فناوری اطلاعات در خصوص مسائل امنیتی دچار تهدیدات بسیاری است. این مخاطرات امنیتی در سطوح مختلف ابر وجود دارد و پرداختن به هر یک از آنها از اهمیت زیادی برخوردار است.

در عین حال، مواردی از جمله، دسترسی تصادفی یا عمدی به اطلاعات، به اشتراک‌گذاری داده‌های حساس و در اختیار گذاشتن اطلاعات سازمان، نبود زیرساخت آنلاین، موجب نگرانی امنیتی سرویس‌گیرندگان است، هرچند که این مسائل را می‌توان با وجود راه‌حل‌های عملی حریم خصوصی و وجود قوانین و مقررات و ایجاد توصیف هویت، فعالیت‌ها، دسترسی‌ها و توافقنامه‌های سرویس حل نمود.

محیط‌های ابری همواره همان تهدیداتی روبرو هستند که شبکه‌های مرسوم شرکت‌ها و سازمان‌ها با آن روبرو هستند. یکی از حجم وسیع داده‌ها و ارائه سرویس‌های اشتراکی، حساسیت این سرویس‌ها چند برابر است. پیچیدگی مسائل امنیتی با توجه به تعدد کاربر و میزان محاسبات بیشتر، بهره‌گیری از کلان داده‌ها نیاز به رویکرد دقیق امنیتی دارد.

رویکردهای جدید نسبت به امنیت نیاز به رویکردی دارد و می‌بایست ریسک‌های مربوطه از جمله، تمرکز ریسک، پیچیده‌تر شدن عملکرد مهاجمان، ریسک‌های درونی و بیرونی که منجر به نشت داده‌ها می‌شود را در بر گیرد و بر آن اساس، تضمین زیرساخت، سخت‌افزار، شبکه، مجازی‌سازی، سیستم‌عامل‌ها، برنامه‌های کاربردی و اجرای سیاست‌های دقیق امنیتی می‌تواند یک نگاه رو به جلو برای کاربرد سریع خدمات ابری جهت ساخت پام‌های امن در محیط‌های ابری را ایجاد نماید. این کتاب به مباحث مهمی از مسائل امنیت ابر، چالش‌های روبرو در پیاده‌سازی رایانش ابری، اجزاء و راه کارهای مورد نیاز در زیرساخت جهت برآورده نمودن الزامات و کنترل‌های امنیتی جدید پرداخته است.

امیدمهدی عبادتی

مشاور فناوری اطلاعات و ارتباطات ریاست دانشگاه

و رییس مرکز تخصصی آپاخورزمی