امنیت داده در رایانش ابری

محمدعلی هادوی

مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت – دانشگاه صنعتی مالک اشتر

hadavi@mut.ac.ir

چشم‌انداز

- مقدمه‌ای بر رایانش ابری
  - تعریف، تاریخچه، لایه‌های خدمت، مدل‌های استقرار
- امنیت در رایانش ابری
  - دیدگاه‌های مختلف در امنیت ابر
  - مرور جنبه‌های امنیتی
  - جمع‌بندی
- موضوعات کارگاه آموزشی
  - پوشش مطالب کارگاه
  - برون‌سپاری امن داده
  - جمع‌بندی

مقدمه‌ای بر رایانش ابری

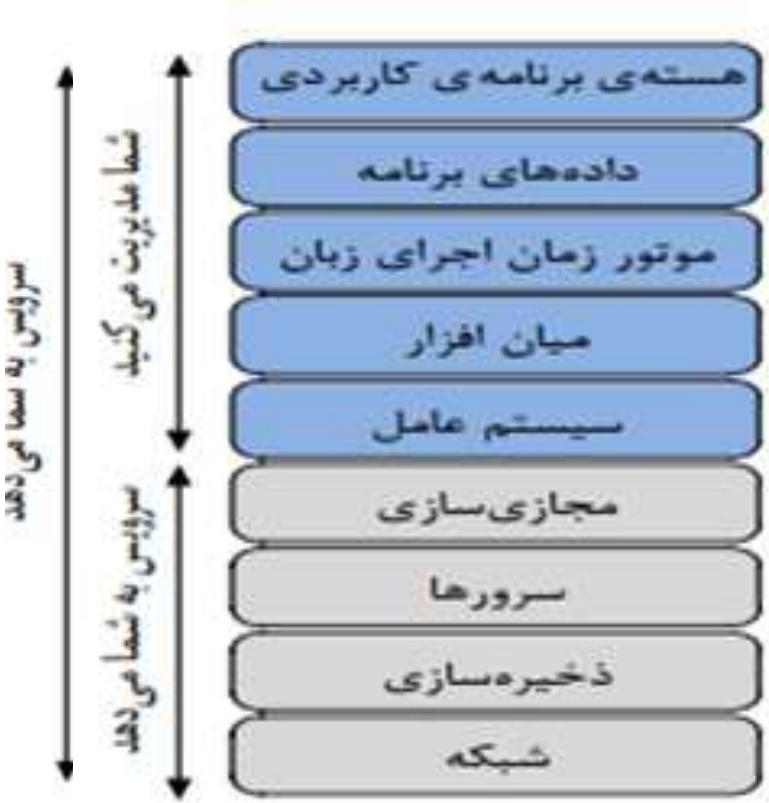
تعریف رایانش ابری

- رایانش ابری مدلی از رایانش است با ویژگی‌های [P. Mull and T. Grance - 2011]
  - دسترس‌پذیری ساده به خدمات از طریق شبکه
  - دسترسی بر اساس تقاضا
  - منابع اشتراکی
  - اخذ و رهاسازی ساده خدمات

تاریخچه‌ی رایانش ابری

- رایانش ابری، امتداد مسیر رایانش توری (Grid Computing)
  - مفهوم مشترک: رایانش در قالب تسهیلات (computing as utility)
  - نقطه‌ی تمایز: مجازی‌سازی
- رایانش ابری، دیدگاه مشابه با ابررایانه‌های قدیمی!
  - ایجاد یک محیط رایانش برای اجرای همزمان سامانه‌های مستقل

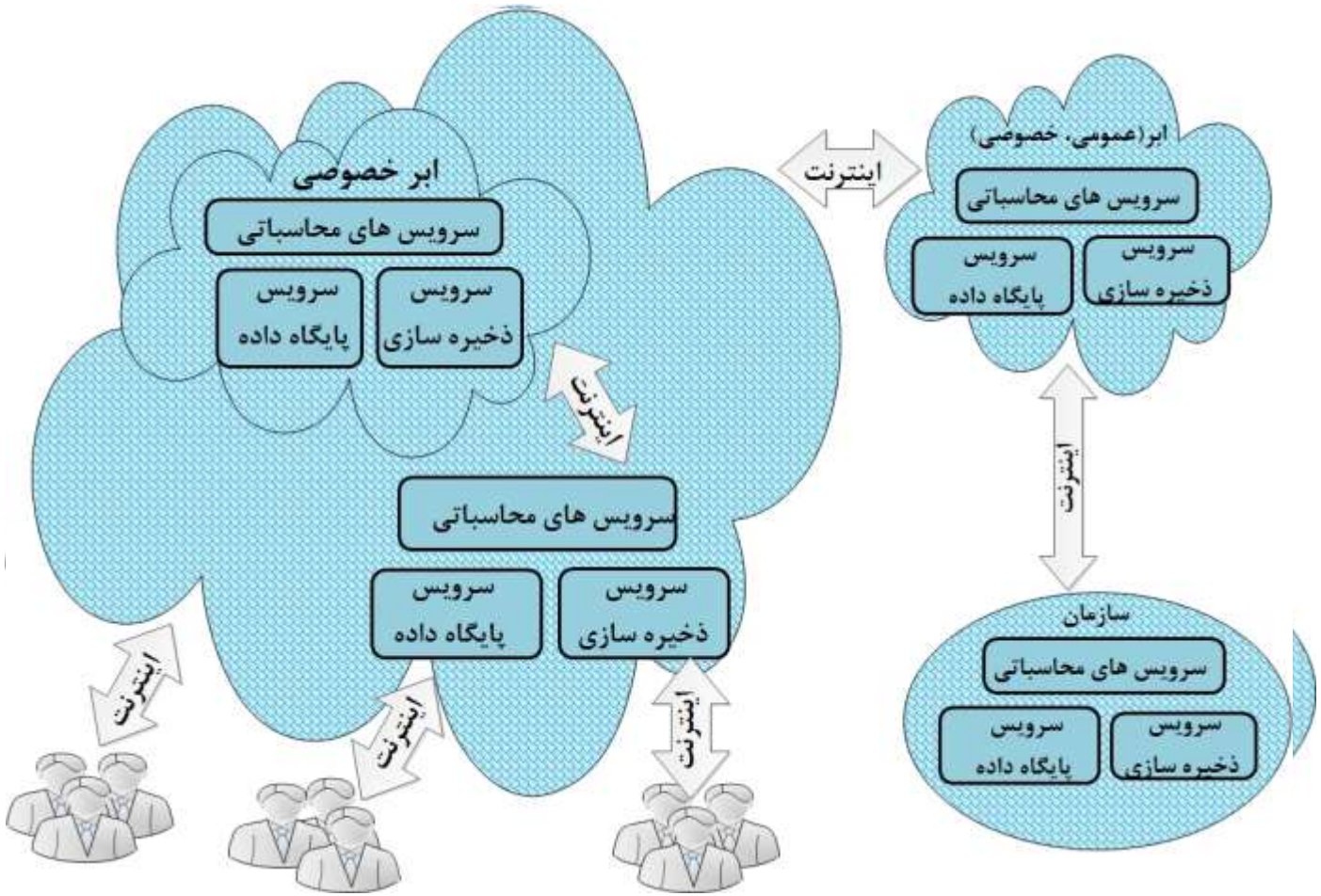
لایه‌های خدمت در رایانش ابری



- **نرم‌افزار به‌عنوان خدمت**
  - Google Docs
- **سکو به‌عنوان خدمت**
  - Google App
- **زیرساخت به‌عنوان خدمت**
  - Amazon EC2 (Elastic Compute Cloud)

مدل‌های استقرار در رایانش ابری

- ابر عمومی
- ابر خصوصی
- ابر گروهی
- ابر ترکیبی



مزایا و معایب رایانش ابری

- ✓ منابع در دسترس
- ✓ کشسانی منابع
- ✓ پرداخت هزینه فقط در صورت نیاز
- ✓ ...
- ✗ امنیت
  - گزارشات متعدد امنیتی
  - کنفرانس‌ها و کارگاه‌های جانبی مرتبط با امنیت ابر
    - ACM Workshop on Cloud Computing Security
    - International Conference on Cloud Security Management
    - SecureCloud

امنیت در رایانش ابری

دیدگاه‌های مختلف در امنیت ابر

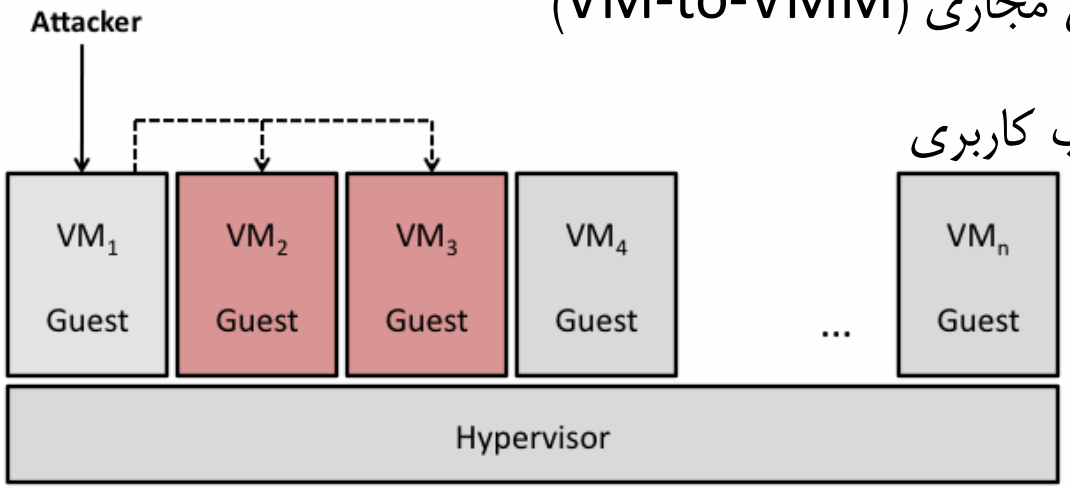
- امنیت با توجه به لایه‌های سرویس‌دهی (نرم‌افزار، سکو و زیرساخت)
- امنیت با عینک ذینفعان ابر (کاربر نهایی، سرویس دهنده و صاحب سرویس)
- ابر مجموعه‌ای از فناوری‌ها (سیستم عامل، اینترنت، نرم‌افزار و ...)
- ابر مجموعه‌ای از مفاهیم (مجازی‌سازی، اعتماد، مفاهیم قانونی/حقوقی و ...)
- جنبه‌های عمومی امنیت در ابر در برابر جنبه‌های اختصاصی
- ...

نرم‌افزار

- جنبه‌های عمومی امنیت نرم‌افزار
  - آسیب‌پذیری‌های نرم‌افزاری
  - زیست‌چرخ امن ایجاد نرم‌افزار
- جنبه‌های امنیت نرم‌افزار ویژه ابر
  - امنیت نرم‌افزار رابط مشتری و ابر
    - دروازه ورود حمله‌کننده

سیستم عامل و شبکه

- جنبه‌های عمومی امنیتی
  - روت‌کیت‌ها، حملات به شبکه و قراردادهای ناامن (حمله فرد میانی، جعل IP، شنود، بدافزارها، و ...)
- جنبه‌های امنیتی ویژه ابر
  - حمله بین مشتریان دارای یک زیرساخت مشترک (cross tenant attacks)
  - حمله دسترسی از ماشین مجازی به ناظر ماشین مجازی (VM-to-VMM)
  - انتشار بدافزار بین تجهیزات مرتبط با یک حساب کاربری



کنترل دسترسی

- جنبه‌های عمومی امنیتی
  - قراردادهای احراز اصالت و حملات به آن‌ها
  - روش‌های مجازشناسی
- جنبه‌های امنیتی ویژه ابر
  - دسترسی غیرمجاز کارمندان داخلی ابر
    - انباشت داده‌های ارزشمند مشتریان و انگیزه برای دسترسی غیرمجاز
  - دسترسی به سرویس‌های متعدد یک سرویس‌دهنده ابری با یک فرایند احراز اصالت متمرکز
    - یک‌بار ورود (Single Sing-On)

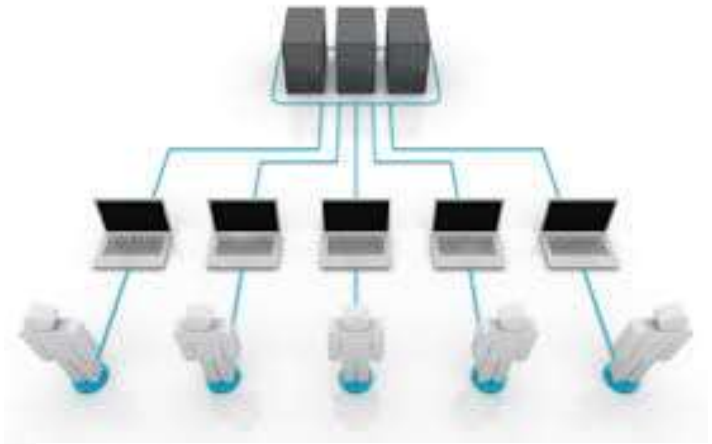
جنبه‌های حقوقی و قانونی

- ماهیت توزیع‌شده داده‌ها
  - پیچیدگی و مسائل حقوقی /قانونی در جرم‌یابی
  - قوانین کشورها در عدم انتقال اطلاعات به خارج از مرزها
- اثر منفی رمزنگاری بر فرایندهایی مانند جرم‌یابی
- فقدان شواهد کافی مرتبط با نقض توافق بین سرویس‌دهنده و سرویس‌گیرنده (SLA)

محاسبه و ذخیره‌سازی

- جنبه‌های عمومی امنیت
  - محرمانگی داده‌ها در ذخیره‌سازی
  - حفظ صحت داده در ذخیره‌سازی و محاسبه
- جنبه‌های امنیتی ویژه ابر
  - مدیریت داده‌های رمز شده بدون دسترسی به کلید
  - اطمینان از عدم دستکاری/فقدان داده در ابر
  - عدم تضمین انتشار/فروش اطلاعات ذخیره شده در ابر
    - (عدم توجه به خطمشی امنیتی صاحب داده)

جمع‌بندی



- دلایل ریشه‌ای مشکلات امنیتی ویژه ابر
  - اشتراک منابع زیرساختی بین مشتریان ابر (multi tenancy)
    - روش‌های جداسازی منابع بین مشتریان آسیب‌پذیر است.
    - آسیب‌پذیری‌ها و تهدیدات عمومی ولی با مخاطره بالاتر در محیط ابر
  - فقدان کنترل ناشی از برون‌سپاری داده و فرایندها
    - عدم اعتماد کامل به کارپذیر ابری
      - ✓ درست‌کار ولی کنجکاو
      - ✓ بالقوه خرابکار

جنبه‌های امنیتی مورد نظر در گارگاه آموزشی

تمرکز مطالب کارگاه آموزشی

- تمرکز بر جنبه‌های امنیتی ویژه ابر در برابر جنبه‌های عمومی امنیتی
- تمرکز بر ناامنی ابر ناشی از فقدان کنترل بر عملکرد آن
- تمرکز بر امنیت داده‌ی برون‌سپاری شده در ابر
- تمرکز بر رویکردهای رمزنگاشتی برای تأمین امنیت داده‌ی برون‌سپاری شده

کاهش مخاطره ناشی از سایر تهدیدات با

ذخیره‌سازی و محاسبه‌ی امن داده‌های برون‌سپاری شده

برون‌سپاری امن داده – بیان مسأله

- سناریوی برون‌سپاری داده
  - برون‌سپاری داده‌ها (مستندات و پایگاه داده) به ابر توسط مالک داده
  - ارائه خدمات مدیریت داده توسط ابر شامل ذخیره‌سازی و محاسبات
    - ابر درست‌کار ولی کنجکاو (و شاید خرابکار!) است.
  - ارسال درخواست‌های جستجو و محاسبات روی داده‌ها توسط کاربران
- نیازمندی‌ها
  - تأمین محرمانگی داده در ابر در عین ارائه خدمات مدیریت داده
  - حفظ حریم خصوصی کاربران
  - اعمال خط‌مشی‌های کنترل دسترسی و تأمین محرمانگی خط‌مشی‌ها
  - اطمینان از صحت پاسخ‌های بازگشتی از ابر

برون‌سپاری امن داده – رویکردهای پاسخ

- جستجو و محاسبه روی داده‌های رمز شده
  - روش‌های رمزنگاری خاص‌منظوره
    - رمزنگاری قطعی
    - رمزنگاری حافظ ترتیب
    - رمزنگاری جستجوپذیر
    - رمزنگاری ویژگی‌بنیاد
    - رمزنگاری همریخت
  - بده–بستان امنیت و کارایی
    - کاربرد فراداده برای جستجو روی داده‌های رمز شده
    - چندپارگی (Fragmentation) داده برای حفظ محرمانگی

جمع‌بندی

- تأمین محرمانگی داده برون‌سپاری شده با رمزگذاری
  - جستجو و محاسبه روی مستندات و داده‌های رمز شده
  - جستجو و محاسبه روی پایگاه داده‌ی رمز شده
- اطمینان از صحت داده‌ی برون‌سپاری شده
  - وارسی درستی پاسخ پرسمان
- تأثیر رمزنگاری بر عملکردهای ابر
  - روش‌های عدم ذخیره‌سازی داده‌های تکراری در ابر
- دیدگاه عملیاتی به ابر
  - برون‌سپاری امن داده و محصولات موجود
  - مدیریت مخاطره در رایانش ابری

مراجع

1. Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Special Publication 800-145, National Institute of Standards and Technology, August 2011, Available at: http://csrc.nist.gov/publications/nistpubs/800-145/sp800-145.pdf
2. Diogo A. B. Fernandes et al. “Security issues in cloud environments: a survey,” Int. J. Inf. Secur, 13(2), April 2014, pp 113–170.
3. E. Aguiar et al., “An Overview of Issues and Recent Developments in Cloud Computing and Storage Security,” pp. 1–31. Springer, Berlin (2013).
4. B. Grobauer et al. “Understanding cloud computing vulnerabilities,” IEEE Secur. Priv. 9(2), 50–57 (2011).
5. D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Gener. Comput. Syst. 28(3), 583–592 (2010).

با تشکر از توجه شما