# Ataques Cibernéticos e Segurança da Computação em Nuvem: Um Guia Completo

*Cyberattacks and Security of Cloud Computing: A Complete Guideline*

Muhammad Dawood Shanshan Tu Chuangbai Xiao Hisham Alasmary Muhammad Waqas Sadaqat Ur Rehman

20 de junho de 2025

Symmetry 2023, Volume 15



Bom dia a todos. Hoje, vamos mergulhar num tema de extrema relevância: a segurança na computação em nuvem. A nossa discussão será baseada no artigo "Ataques Cibernéticos e Segurança da Computação em Nuvem: Um Guia Completo". O objetivo é fornecer uma visão abrangente sobre os desafios e as soluções nesta área vital da tecnologia.

## Sumário





Aqui está a estrutura da nossa apresentação. Começaremos com uma introdução à computação em nuvem, seguida pelos seus modelos de serviço e implantação. Depois, abordaremos os principais problemas de segurança e os ataques mais comuns. Em seguida, discutiremos as soluções e contramedidas e, por fim, concluiremos com as direções futuras da área.

# Introdução à Computação em Nuvem

## O que é a Computação em Nuvem?

- Uma técnica inovadora que oferece recursos compartilhados para armazenamento e gerenciamento de servidores.
- Transforma soluções tecnológicas para sistemas de grande escala em frameworks de ”servidor como serviço”.
- Benefícios chave:
  - Redução de custos
  - Flexibilidade e escalabilidade
  - Alta disponibilidade
  - Serviço sob demanda
- No entanto, essa tecnologia também abre portas para novas ameaças e problemas de segurança.



Vamos começar por definir o que é a computação em nuvem. Essencialmente, é um modelo que nos permite aceder a recursos computacionais partilhados pela internet. Ela revolucionou a forma como as empresas gerem a sua infraestrutura de TI, oferecendo benefícios como redução de custos, grande flexibilidade e a capacidade de escalar recursos conforme a necessidade. Contudo, como veremos, esta conveniência traz consigo novos e complexos desafios de segurança.

## Objetivos do Estudo

- Discutir os diferentes modelos e serviços de nuvem.
- Analisar as tendências de segurança e os problemas associados.
- Propor contramedidas específicas para os ataques identificados.
- Apontar direções futuras para a pesquisa em segurança na nuvem.

Os objetivos desta apresentação, alinhados com o artigo, são claros. Primeiro, vamos entender os blocos de construção da nuvem. Em seguida, identificaremos onde estão as vulnerabilidades. Depois, exploraremos como podemos nos defender. E, finalmente, olharemos para o futuro para antecipar os próximos desafios.

# Modelos e Serviços

## Modelos de Serviço

**IaaS** *(Infrastructure as a Service)*

- Recursos fundamentais.
- VMs, servidores, armazenamento.
- **Desafio:** Segurança de VMs e hipervisores.

**PaaS** *(Platform as a Service)*

- Ambiente para desenvolvimento.
- **Desafio:** Proteger dados sensíveis processados pela plataforma.

**SaaS** *(Software as a Service)*

- Aplicações via internet.
- **Desafio:** Privacidade dos dados em ambientes compartilhados.



A nuvem oferece serviços em três modelos principais. IaaS, ou Infraestrutura como Serviço, fornece os blocos de construção básicos, como máquinas virtuais. Aqui, o grande desafio é proteger a própria infraestrutura virtual. PaaS, ou Plataforma como Serviço, oferece um ambiente para os developers criarem aplicações, e o foco da segurança é proteger os dados que a plataforma manipula. Por último, SaaS, ou Software como Serviço, entrega aplicações prontas a usar, e a principal preocupação é garantir a privacidade dos dados dos utilizadores.

## Modelos de Implantação

- **Nuvem Privada:**
  - Operada para uma única organização.
  - Maior controle e segurança.
  - **Desafio:** Ameaças internas e gestão robusta de acessos.
- **Nuvem Pública:**
  - Recursos oferecidos ao público geral (ex: AWS, Azure).
  - **Desafio:** Proteger dados em ambiente compartilhado (multitenancy).
- **Nuvem Híbrida:**
  - Combinação de duas ou mais nuvens (privada, pública).
  - **Desafio:** Coordenar a segurança entre diferentes domínios.
- **Nuvem Comunitária:**
  - Para um grupo de instituições com necessidades comuns.
  - **Desafio:** Balancear requisitos de segurança de múltiplos membros.



Além dos modelos de serviço, temos os modelos de implantação. A Nuvem Privada oferece o máximo controlo, mas é vulnerável a ameaças internas. A Nuvem Pública, a mais comum, tem o desafio do "multitenancy", ou seja, partilhar recursos de forma segura. A Nuvem Híbrida combina o melhor dos dois mundos, mas a sua complexidade torna a segurança um desafio de coordenação. Por fim, a Nuvem Comunitária serve a grupos específicos, onde o desafio é harmonizar as políticas de segurança de todos os membros.

# Principais Problemas de Segurança

## Problemas Fundamentais

- **Violação de Dados (Data Breaches):** Divulgação não autorizada de informação sensível.
- **Confidencialidade dos Dados:** Garantir que os dados não sejam revelados a usuários não autorizados.
- **Controle de Acesso:** Restringir o acesso aos dados apenas a usuários legítimos.
- **Autenticação:** Processo de verificação da identidade do usuário.
- **Phishing:** Engenharia social para obter informações confidenciais.
- **Exposição de Chaves:** Risco de chaves de criptografia serem comprometidas.
- **Auditoria e Privacidade:** Necessidade de revisar e investigar a infraestrutura, protegendo a identidade do usuário.



Agora, vamos focar-nos nos problemas de segurança. A violação de dados é talvez a mais temida. Intimamente ligadas a isso estão a confidencialidade e o controlo de acesso. A autenticação fraca é uma porta de entrada comum para atacantes, muitas vezes através de técnicas de phishing. A exposição de chaves criptográficas pode inutilizar todas as outras medidas de segurança. E, finalmente, a auditoria é crucial para verificar a conformidade, mas deve ser feita preservando a privacidade.

## Problemas de Virtualização

- **Isolamento de VMs:** Múltiplas Máquinas Virtuais (VMs) partilham o mesmo host físico, aumentando o risco de ataques entre VMs.
- **Hipervisor (Hypervisor):** Uma falha no hipervisor pode comprometer todo o sistema host e as VMs convidadas.
- **Migração de VMs:** A transferência de VMs entre hosts pode ser interceptada se a conexão não for criptografada (ataque Man-in-the-Middle).
- **Malware Específico:** Formas de malware que visam a virtualização e não são detetadas por antivírus tradicionais.



A tecnologia de virtualização, que é a base da nuvem, traz os seus próprios desafios. O isolamento inadequado entre Máquinas Virtuais pode permitir que um atacante numa VM afete outras. O hipervisor, o software que gere as VMs, é um ponto único de falha de alta criticidade. A migração de VMs, um processo comum para balanceamento de carga, pode expor dados se não for devidamente protegida. E já existem malwares desenhados especificamente para atacar estes ambientes virtualizados.

# Ataques Comuns na Nuvem

## Tipos de Ataques

- **Negação de Serviço (DoS/DDoS):**
  - Objetivo: Tornar os serviços indisponíveis para usuários legítimos.
  - DDoS utiliza múltiplas fontes para dificultar a mitigação.
- **Ataque Sybil:**
  - O atacante cria múltiplas identidades falsas para ganhar uma influência desproporcional na rede.
- **Ataque de Buraco Negro (Black Hole):**
  - Um nó malicioso atrai todo o tráfego de rede, mas descarta os pacotes em vez de os encaminhar.
- **Ataque de Buraco de Minhoca (Wormhole):**
  - O atacante cria um túnel de baixa latência entre dois pontos da rede para analisar ou modificar o tráfego.



Vamos analisar alguns ataques específicos. Os ataques de Negação de Serviço, ou DoS, visam sobrecarregar os sistemas e torná-los inacessíveis. No ataque Sybil, um atacante cria identidades falsas para manipular a rede. Num ataque de Buraco Negro, um nó malicioso atrai o tráfego e simplesmente o descarta, criando uma falha de comunicação. E no ataque de Buraco de Minhoca, o atacante cria um atalho na rede para interceptar ou analisar o tráfego de forma invisível.

# Soluções e Contramedidas

## Estratégias de Defesa

- **Autenticação Multifator (MFA):** Adiciona camadas extras de verificação para além da senha, dificultando o acesso não autorizado.
- **Criptografia Robusta:** Proteger os dados em repouso (armazenados) e em trânsito (durante a comunicação).
- **Sistemas de Deteção de Intrusão (IDS):**
  - **NIDS:** Baseado em rede.
  - **HIDS:** Baseado em host.
  - **IDS baseado em Hipervisor:** Monitoriza a comunicação entre VMs.
- **Gestão de Credenciais e Acesso (IAM):** Garantir que apenas indivíduos autorizados acedam aos recursos necessários.
- **Honeypots:** Sistemas "isca"projetados para atrair, detetar e analisar o comportamento de atacantes.



Felizmente, temos um arsenal de estratégias de defesa. A Autenticação Multifator é uma das formas mais eficazes de proteger contas. A criptografia é fundamental para proteger os dados onde quer que eles estejam. Os Sistemas de Deteção de Intrusão atuam como alarmes, monitorizando a rede, os sistemas e até mesmo o hipervisor. A Gestão de Acesso, ou IAM, garante que o princípio do menor privilégio seja aplicado. E os Honeypots são ferramentas inteligentes para estudarmos os nossos adversários.

## Técnicas Avançadas

- **Abordagem Auto-Adaptativa:** Utiliza monitorização em tempo real para detetar desvios de comportamento e adaptar as defesas.
- **Assinaturas em Anel (Ring Signatures):** Permitem validar metadados para monitorizar a integridade de dados partilhados, mantendo o anonimato do signatário.
- **Auditoria em Tempo de Execução:** Framework para auditar a segurança ao nível do usuário, como controle de acesso compartilhado.
- **Chaves de Revogação:** Permitem que a nuvem invalide blocos de dados associados a um usuário revogado de forma eficiente.



Além do básico, existem técnicas mais avançadas. Sistemas auto-adaptativos podem responder a ameaças dinamicamente. As Assinaturas em Anel são uma técnica criptográfica que permite a verificação anónima, útil para a integridade de dados partilhados. A auditoria em tempo de execução permite uma verificação contínua das políticas de segurança. E as chaves de revogação são cruciais para gerir eficientemente o ciclo de vida dos utilizadores e dos seus acessos.

# Direções Futuras e Conclusões

## Tópicos em Aberto e Pesquisas Futuras

- **Criptografia Homomórfica:** Realizar computações sobre dados criptografados sem a necessidade de os descriptografar.
- **Machine Learning (ML):** Usar IA e ML para deteção avançada de ameaças e anomalias.
- **Computação em Névoa (Fog Computing):** A segurança precisa ser adaptada para este paradigma emergente que aproxima a computação dos dispositivos IoT.
- **Deteção de Ameaças Internas (Insider Threats):** Desenvolver soluções padronizadas para distinguir usuários normais de insiders maliciosos.
- **Desduplicação Segura:** Mecanismos eficientes de desduplicação para backups nuvem-a-nuvem que preservem a segurança.



Olhando para o futuro, a pesquisa em segurança na nuvem foca-se em áreas fascinantes. A Criptografia Homomórfica promete ser um divisor de águas para a privacidade. O Machine Learning está a tornar-se indispensável para detetar ameaças cada vez mais sofisticadas. A ascensão da Fog Computing e da IoT traz novos desafios de segurança. A deteção de ameaças internas continua a ser um problema difícil. E a desduplicação, uma técnica de otimização de armazenamento, precisa de ser feita de forma segura.

## Conclusões

- A computação em nuvem oferece enormes vantagens, mas a segurança continua a ser um desafio crítico.
- Uma abordagem de segurança em várias camadas é essencial, combinando prevenção, deteção e resposta.
- O cenário de ameaças está em constante evolução, exigindo pesquisa e desenvolvimento contínuos de novas contramedidas.
- A colaboração entre academia e indústria é fundamental para construir um ecossistema de nuvem mais seguro e confiável.



Para concluir: a nuvem é poderosa, mas a sua segurança é uma responsabilidade partilhada e um desafio constante. Não existe uma solução única; precisamos de uma defesa em profundidade. O campo está sempre a mudar, por isso a inovação contínua é vital. E, mais importante, o progresso real virá da colaboração entre pesquisadores, empresas e a comunidade de segurança em geral.

# Obrigado!

Perguntas?



Muito obrigado pela vossa atenção. Agora, gostaria de abrir o espaço para quaisquer perguntas que possam ter.