Relação custo/benefício de técnicas utilizadas para prover privacidade em computação nas nuvens

AUTORES: VITOR HUGO GALHARDO MOIA

MARCO AURÉLIO AMARAL HENRIQUES

APRESENTADOR: MÁRCIO LUÍS PETRY

Sumário

- Introdução
  - Motivação
  - Objetivos
- Problemas relacionados a privacidade na nuvem
- Análise do custo/benefício das soluções
- Conclusão

Introdução

- Computação nas nuvens:
  - –Opção para armazenamento de dados:
    - Escalável
    - Dinâmica
    - Grande disponibilidade dos dados
    - Pagamento sob demanda
    - Evita-se custos de infraestrutura e manutenção locais

Motivação

- Preocupação com a segurança e privacidade na nuvem:
  - Dados normalmente armazenados em claro.
  - Potencial acesso a informações sensíveis pelos provedores.
  - Falhas na segurança da infraestrutura que permitam a invasores se apoderar de dados armazenados.

Objetivos

- Discutir os principais problemas relativos ao sigilo dos dados na nuvem e métodos para resolvê-los.

- Realizar estimativas dos custos e benefícios de cada método para uma comparação entre os mesmos.

Problemas relacionados a privacidade na nuvem

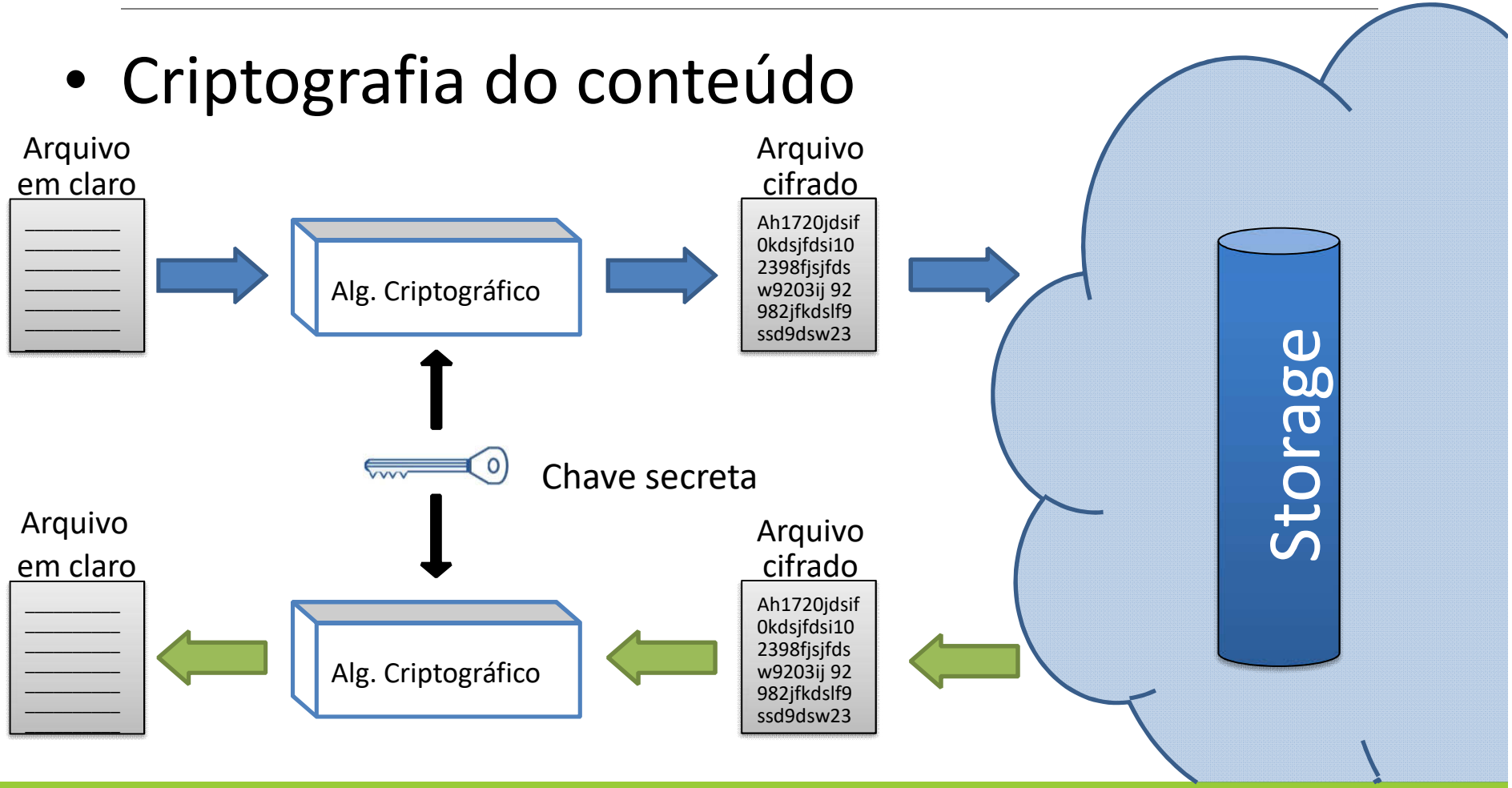
- Sigilo do conteúdo
- Sigilo do nome dos dados
- Sigilo de localização durante acesso aos dados
- Sigilo sobre a posse de um dado

Sigilo do conteúdo

- Restringe acesso aos dados.
- Usuários não precisam confiar em seus provedores de serviço cegamente.
- Proteção contra atacantes externos.
- Possíveis soluções:
  - Criptografia do conteúdo
  - Fragmentação dos dados

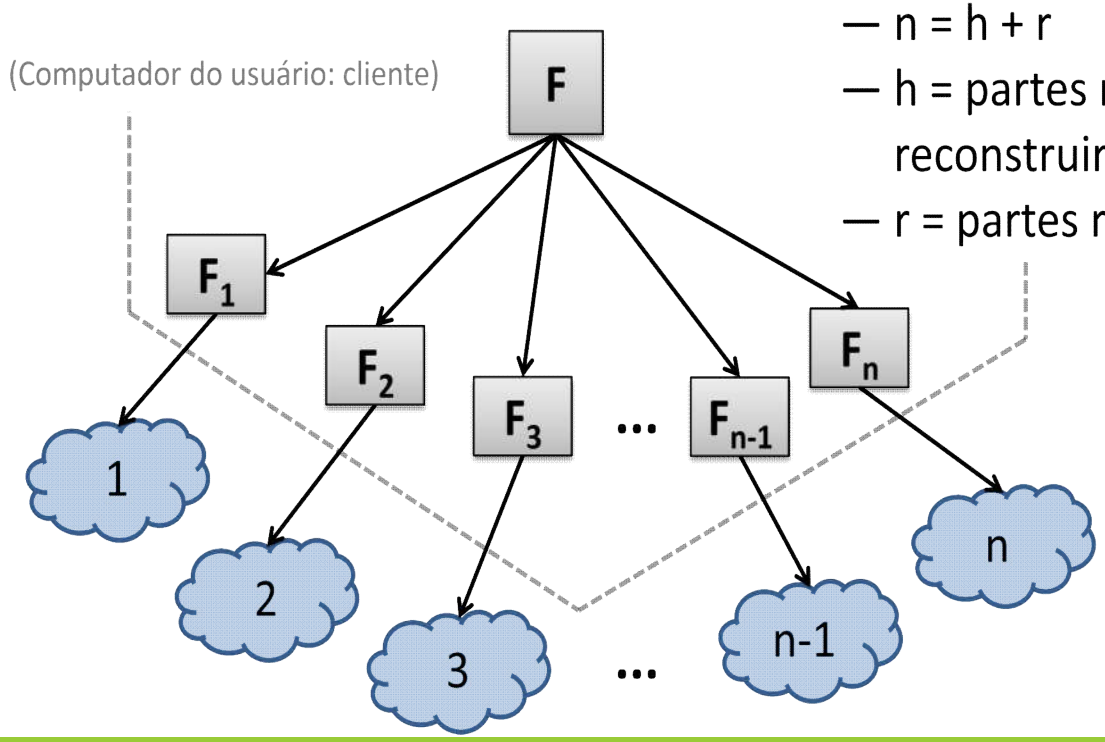
Sigilo do conteúdo (Cont.)

- Criptografia do conteúdo



Sigilo do conteúdo (Cont.)

• Dados são fragmentados (com ou sem redundância) e fragmentos são armazenados em diferentes nuvens



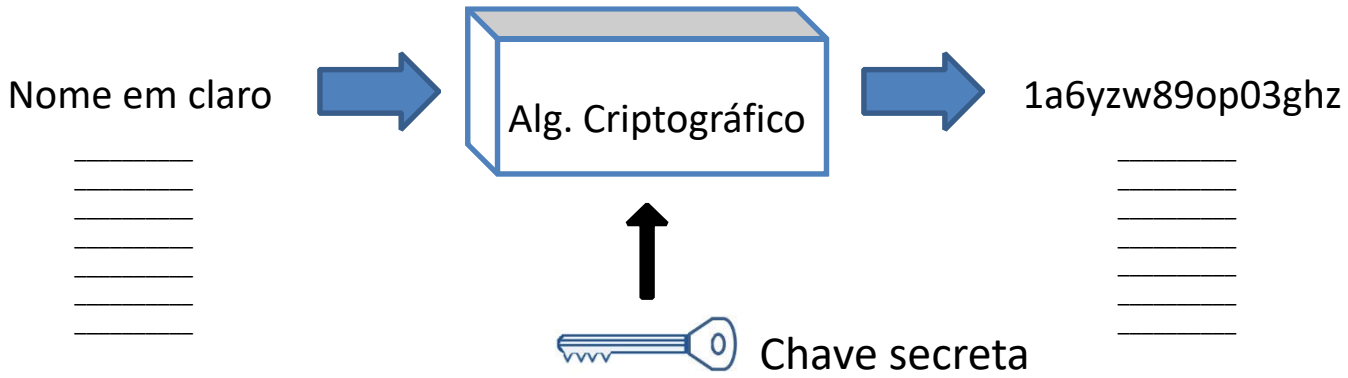
— n = h + r
— h = partes necessárias para reconstruir o dado original
— r = partes redundantes

Sigilo do nome dos dados

- Nome ou extensão do dado pode:
  - Revelar informações relativas a seu conteúdo.
    - Ex: extrato_20150330.
  - Revelar fragmentação.
    - Ex: dado-parte1, dado-parte2 etc.
- Possível solução:
  - Criptografia do nome

Sigilo do nome dos dados (Cont.)

- Criptografia do nome

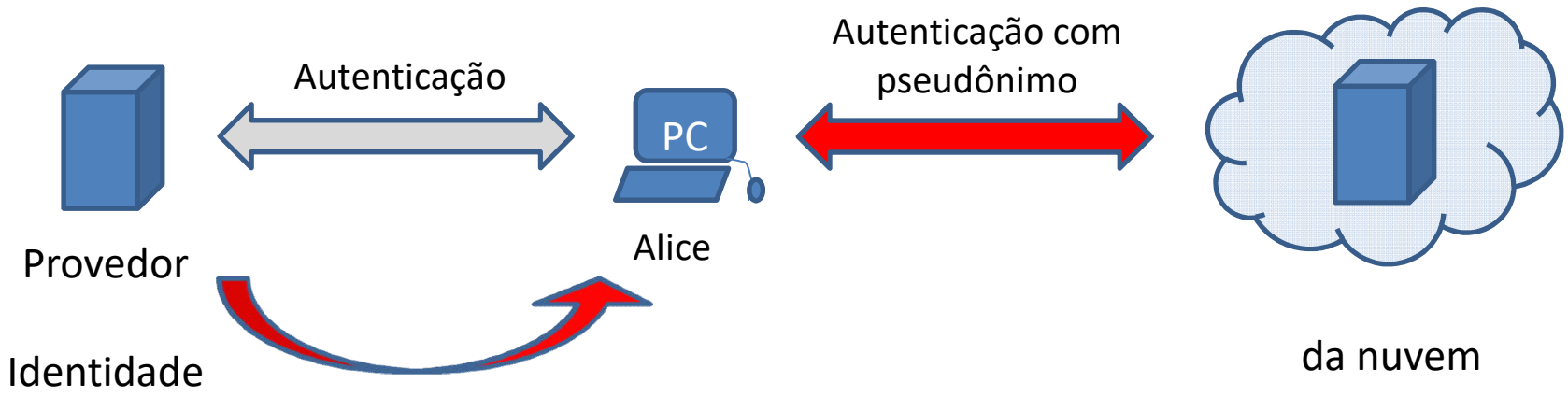


Sigilo de localização durante acesso aos dados

- Localização (IP) do usuário pode ser uma informação sensível
- Possíveis formas de ocultar localização:
  - VPN-Proxy
  - TOR

Sigilo sobre a posse de um dado

- Ligação dos dados a seus respectivos donos pode ser problemática.
- Possível solução:
  - Autenticação terceirizada (OpenId, Shibboleth etc)



Análise do custo/benefício das soluções

- *CR* = Custo relativo -> Estimativa do custo em termos de tempo.
- *PR* = Privacidade relativa -> Estimativa do nível de privacidade

Sigla	Técnica
T_5	Criptografar conteúdo
T_4	Fragmentar com redundância
T_3	Ocultar acesso via TOR
T_2	Ocultar acesso via VPN-Proxy
T_1	Ocultar posse dos dados (identidade federada)
T_0	Ocultar nome dos dados (criptografia de nomes)

Análise do custo/benefício das soluções (Cont.)

- Possibilidade de 48 combinações das técnicas.
- Código binário para representar cada solução
  - Cada técnica possui uma posição em uma palavra de 6 bits.
  - 0 (não utilização) e 1 (utilização) de determinada técnica.
  - Ordem: *T5, T4, T3, T2, T1, T0*.
  - Valor decimal resultante representa a solução.
- Ex: Cript. Conteúdo (T5) + frag. (T4) + TOR (T3) =111000 = 56

Análise do custo/benefício das soluções (Cont.)

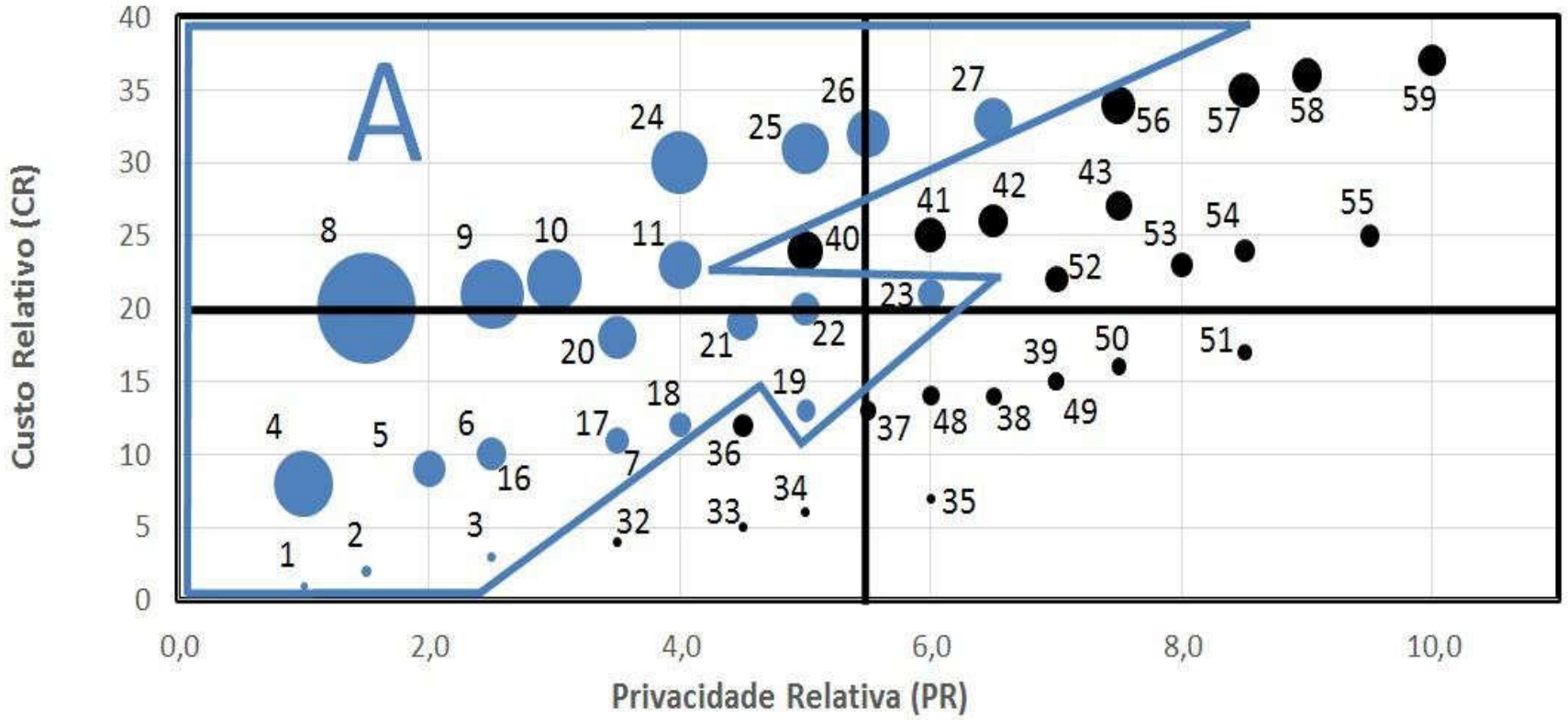
- *Ri = CRi / PRi*

– *CRi* e *PRi* de uma combinação *i* são influenciados pelos *PR* e *CR* de cada uma de suas técnicas.

- Cenário: download de um arquivo de 10MB

Sigla	Técnica	CR	PR
T_5	Criptografar conteúdo	04	3,5
T_4	Fragmentar com redundância	10	2,5
T_3	Ocultar acesso via TOR	20	1,5
T_2	Ocultar acesso via VPN-Proxy	08	1,0
T_1	Ocultar posse dos dados (identidade federada)	02	1,5
T_0	Ocultar nome dos dados (criptografia de nomes)	01	1,0

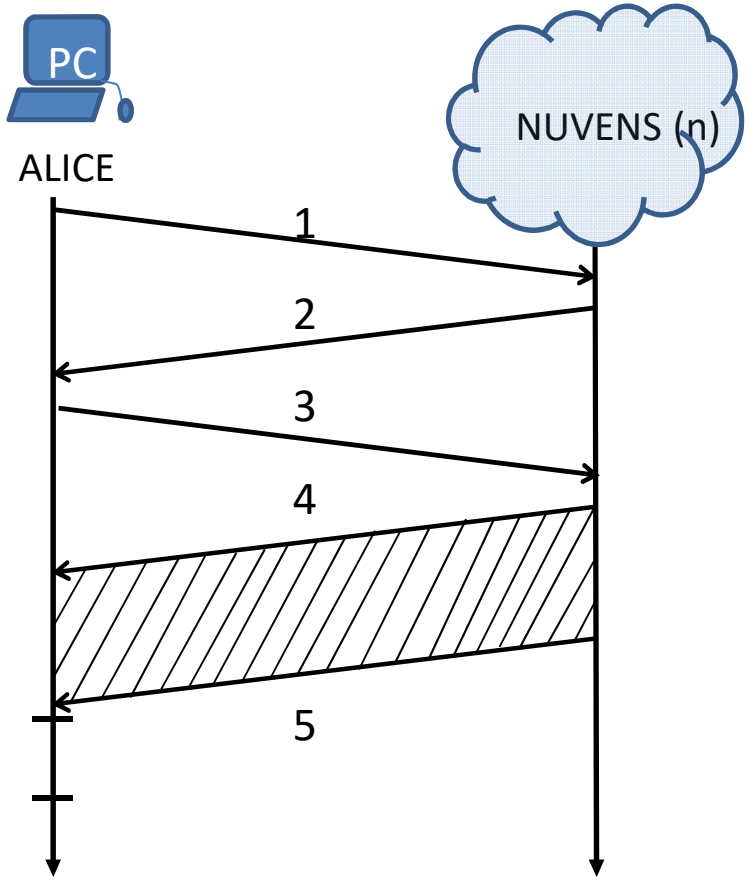
Custo/benefício das soluções (estimativas iniciais aproximadas)



Custo/benefício das soluções (estimativas melhoradas)

Sigla	Técnica	CR	PR
T_5	Criptografar conteúdo	4,71	10
T_4	Fragmentar com redundância	1,00	4
T_3	Ocultar acesso via TOR	9,67	5
T_2	Ocultar acesso via VPN-Proxy	2,48	3
T_1	Ocultar posse dos dados (identidade federada)	2,41	2
T_0	Ocultar nome dos dados (criptografia de nomes)	2,37	1

Fragmentação

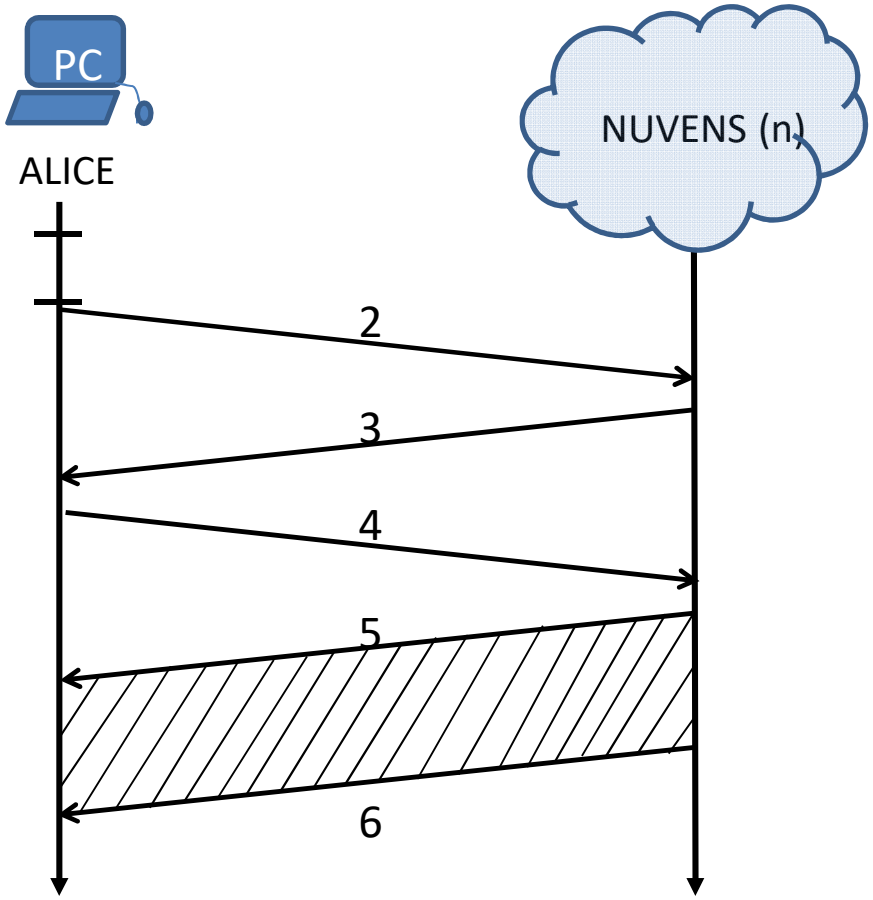


1 – Envia credencial p/ login
2 – Confirma login
3 – Pede fragmento arquivo
4 – Recebe início frag. arquivo
5 – Recebe fim frag. arquivo
6 – Junta fragmentos

Tempo gasto:

$T = (3*T_{msgcurta}) + (T_{prop} + (nº\ msg\ arq\ frag * T_{transmissão})) + T_{juntarfrag}$

Sigilo no Nome

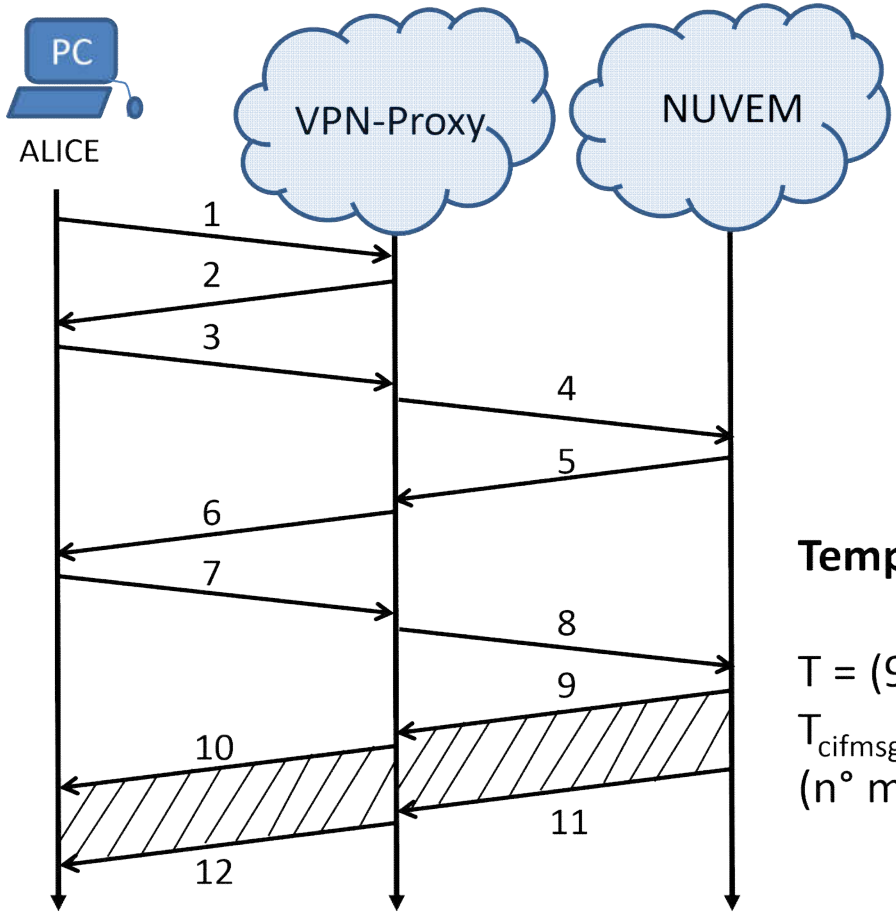


1 – Cifrar nome do arquivo
2 – Envia credencial p/ login
3 – Confirma login
4 – Pede arquivo (nome cifrado)
5 – Recebe início arquivo
6 – Recebe fim arquivo

Tempo gasto:

$T = T_{cifnome} + (3 * T_{msgcurta}) + T_{prop} + (n° \text{ msg arquivo} * T_{transmissão})$

VPN-Proxy



1 – Pede conexão segura
2 – Estabelece canal seguro
3, 4 - Envia credencial p/ login
5, 6 - Confirma login
7, 8 - Pede arquivo
9, 10 – Recebe início arquivo
11, 12 – Recebe fim arquivo

Tempo gasto:

$T = (9*T_{msgcurta}) + (3*T_{msgcurtacif}) + T_{cifmsglong} + (n° \text{ msg arquivo}*T_{decifmsglonga})$

Conclusão

- Este trabalho apresentou uma estimativa da relação custo/benefício de soluções para minimizar problemas de sigilo e privacidade de arquivos armazenados em nuvens.

- Os resultados mostram que algumas soluções podem ser ineficientes e até proibitivas.

Trabalhos Futuros

- Obter estimativas mais precisas dos custos e benefícios de forma a se ter uma visão mais completa que permita uma melhor tomada de decisão sobre que solução utilizar.
- Buscar formas mais adequadas para se determinar o nível de privacidade relativa na visão do usuário.

Referências

• Abu-Libdeh, H., Princehouse, L., and Weatherspoon, H. (2010). Racs: A case for cloud storage diversity. In Proc. of ACM, SoCC ’10, pages 229–240, New York, NY, USA. ACM.
• Duffield, N., Greenberg, A., Goyal, P., Mishra, P., Ramakrishnan, K., and Van der Merwe, J. (2005). Virtual private network. US Patent 6,912,232.
• Murdoch, S. and Danezis, G. (2005). Low-cost traffic analysis of tor. In Security and Privacy, 2005 IEEE Symposium on, pages 183–195.
• Padmaja, N. and Koduru, P. (2013). Providing data security in cloud computing using public key cryptography. IJESR, 4(01).
• Schnjakin, M., Alnemr, R., and Meinel, C. (2011). A security and high availability layer for cloud storage. In Proc. of, WISS’10, pages 449–462, Berlin, Heidelberg. Springer-Verlag.