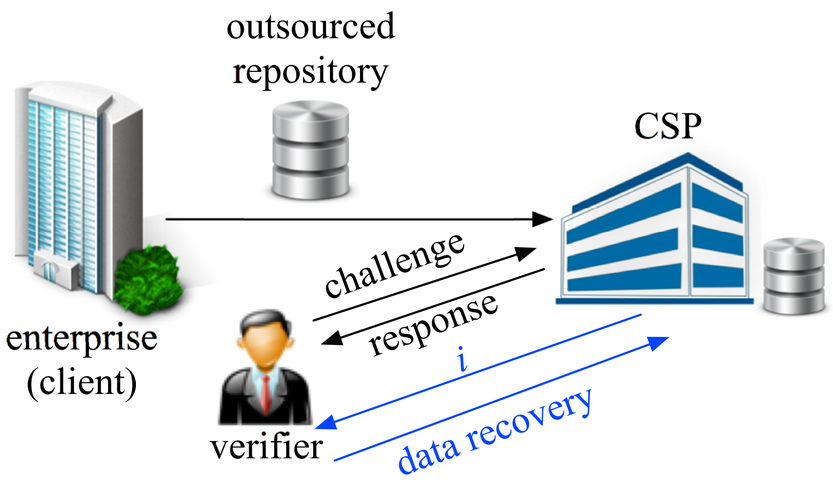
SaTC: CORE: Small: Secure Cloud Storage Verification Methods

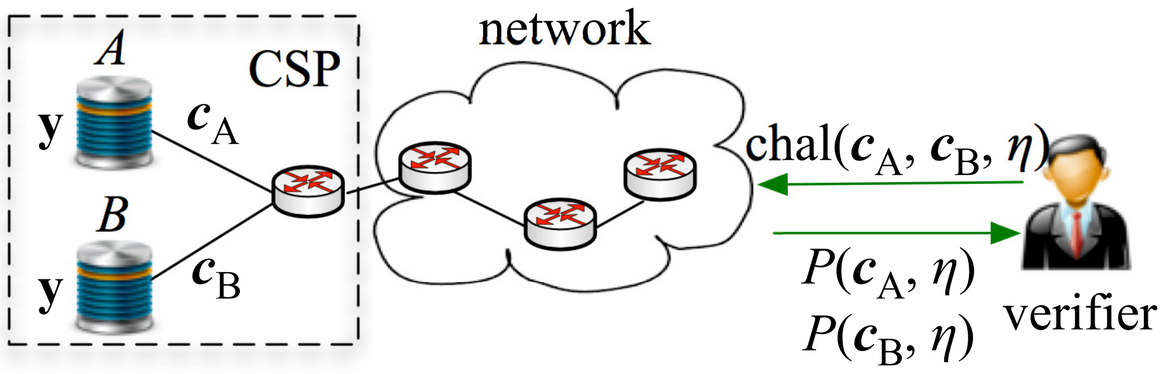
Loukas Lazos, Marwan M Krunz, Bane Vasic, The University of Arizona
https://cloudsec.ece.arizona.edu/

THE UNIVERSITY OF ARIZONA

Project Goal: Design and test auditing mechanisms for provably and efficiently verifying fault-tolerance in cloud repositories



Verification of redundancy



Verification of physical storage diversity

Main Challenges:

- Cloud Storage Providers (CSPs) are in full control of outsourced data and can store it in less reliable ways
- Verifying fault-tolerance is non-trivial because redundant data can be computed on-the-fly
- Physical storage redundancy is even more challenging because it relates to verifying physical properties such as distinction between storage devices

Scientific Impact:

- Developed Proof-of-Reliability (PoRL) methods that can be used for checking the degree of fault-tolerance
- PoRL methods generalize to data integrity checks at low communication overhead
- Efficient data recovery from data loss and confidentiality are maintained
- Novel timing methods for verifying physical storage diversity

A PoRL Construct

f consists of t symbols $\mathbf{f} = (f_1, f_2, \ldots, f_t)$

f $[f_1][f_2]\cdots[f_t]$

1. Insert $k - t$ pseudo-random verification symbols

m $[m_1][m_2]\cdots[m_k]$

2. Apply $(n, k, d, r)_q$ ECC code

c $[c_1][c_2]\cdots[c_k]\cdots[c_n]$

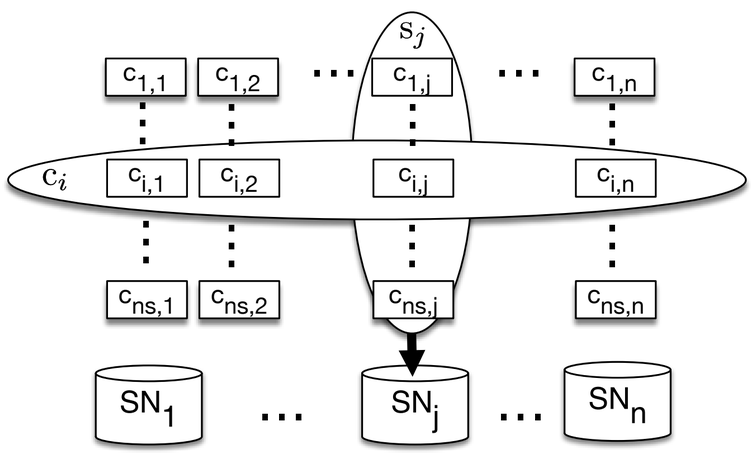
3. Create noise vector **e** and add it to **c**

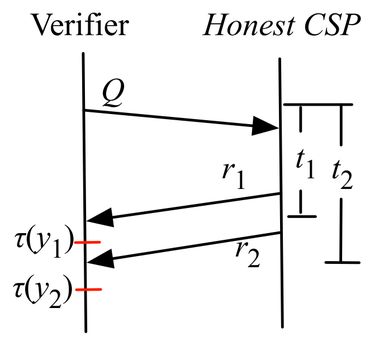
y $[\quad][\quad]\cdots[\quad]$ with y_1, y_2, y_n

4. Break **y** into n_s subfiles of size n/n_s

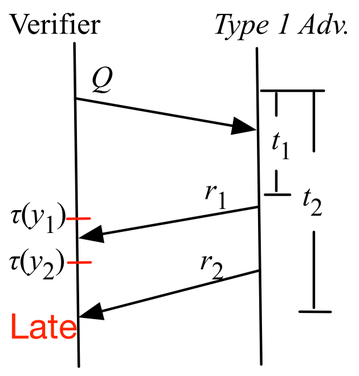
y $[\cdots][\cdots]\cdots[\cdots]$ with y_1, y_{ns}

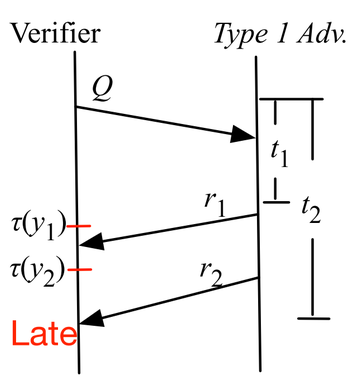
Storage Layout Across Storage Nodes for storage diversity verification





Timing Tests





Broader Impact:

- Mitigate risk of data loss, improve fault-tolerance of cloud storage, discover misconfigurations, and combat poor storage practices
- Enable auditability of service level agreements from data owners and third parties while preserving data confidentiality

Education and Outreach:

- Research results have been integrated to two graduate courses and one undergraduate course
- PIs have promoted research outcomes in outreach events in UA STEM initiatives and the WISE program

Broader Impact and Broader Participation:

- The project has partially supported three female PhD students
- Led to 20+ publications so far
- Results disseminated with 15+ presentations