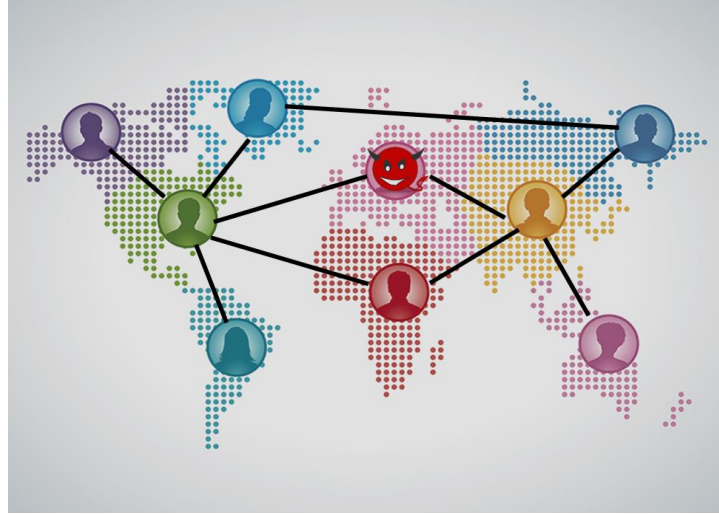


Secure Collaborations with Additive Splits

Siva C. Chaduvula, Bijeeta Pal, Mikhail J. Atallah, Jitesh H. Panchal
Purdue University

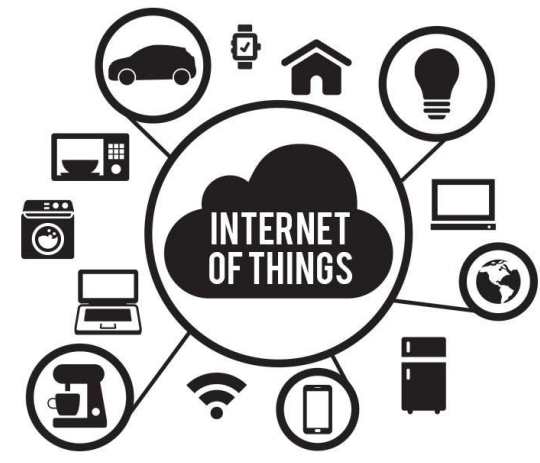
Collaborations are increasingly becoming complex

- Collaborations across enterprise/national boundaries
- Common collaborator among competing enterprises
- Collaborator is a future competitor



Are your collaborators trustworthy?

- Limitations of existing multi-party computations (MPC)
 - Trusted Third Party → Prone to information leakage
 - Fully Homomorphic Encryption
 - Secure Circuit Evaluation
- Value creation in Internet of Things (IoT) environment
 - Real time data analysis
 - Limited power of sensors/actuators
 - Might involve privacy (for e.g. cameras)



How to achieve MPC swiftly, securely and economically?

Cloud storage-Need and Trend of today



- Companies don't want to spend money and resource in building and maintaining data storage. Cloud servers are an economical solution
- But is it safe to give your private data to cloud servers?
- All the communication and storage is in encrypted form. Looks safe

Issues



A rogue employee can learn the data

Update can be difficult if file is encrypted



Hacker somehow gets the encryption key

Deletion from the cloud is not in your hand



Cloud service provider decides to disclose your data to third party

Secure Computation

Online Auctions

- Buyer does not want to reveal item quantities
- Vendors do not want to reveal item prices

Buyer

- Inputs**
- Item names
 - Item quantities
- Outputs**
- Item winners
 - Payments



Vendors

- Inputs**
- Item names
 - Item prices
- Outputs**
- Items won
 - Payment

Confidentiality Preservation

- Buyer cannot learn winning item price
- Losing bids are never revealed to anyone
- Cloud servers learn nothing

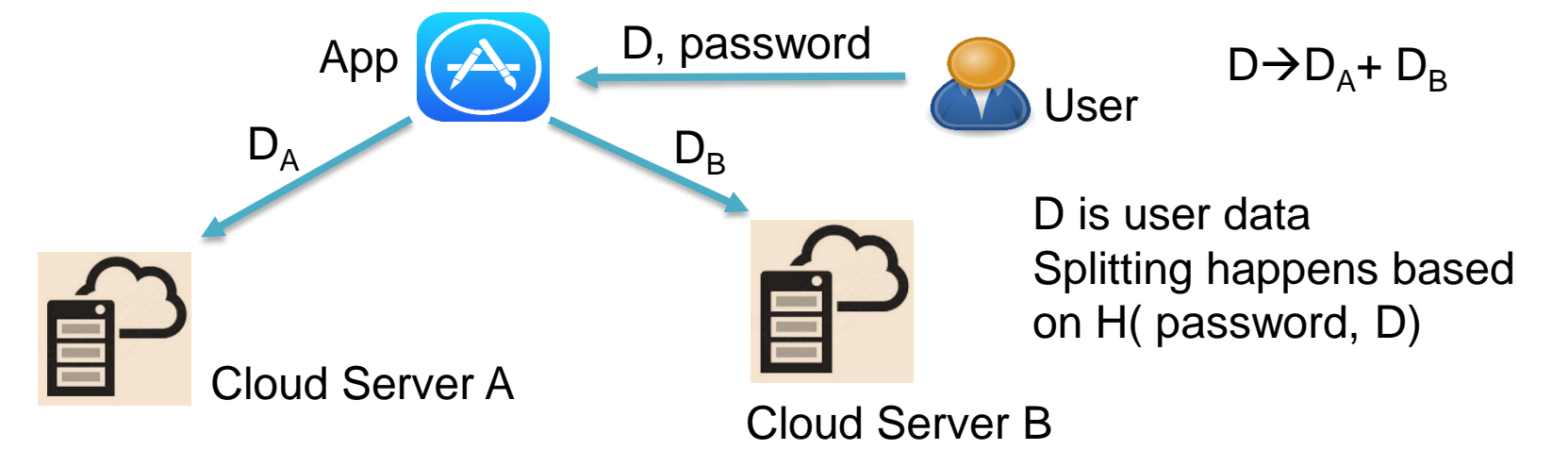
Additive splits (AS) based protocol framework

Step #	Action	Alice and Bob want to compute $H(U,V)$
1	Split with a local seed(L) and share among collaborators	$V = V_a + V_b$ $V_a = \frac{V}{2} - R_L$ $V_b = \frac{V}{2} + R_L$ Alice: A Bob: B $U = U_a + U_b$
2	Mask the shares by a shared seed(S)	$M_{La} = f_1(U_a, R_s)$ $M_{Lb} = f_1(U_b, R_s)$ $M_{Va} = f_2(V_a, R_s)$ $M_{Vb} = f_2(V_b, R_s)$
3	Send to a semi-honest server	M_{La}, M_{Va} M_{Lb}, M_{Vb} Semi-honest Server
4	Server computes on masked splits	$O = g(M_{La}, M_{Lb}, M_{Va}, M_{Vb})$ $U \neq M_{La} + M_{Lb}$ $V \neq M_{Va} + M_{Vb}$
5	Server splits the outcome with a local seed and sends the shares to collaborators	O_a O_b $O = O_a + O_b$
6	Collaborators undo masking on the received shares	$H(U,V) = H_a + H_b$ $H_a = f_1^{-1} f_2^{-1}(O_a)$ $H_b = f_1^{-1} f_2^{-1}(O_b)$

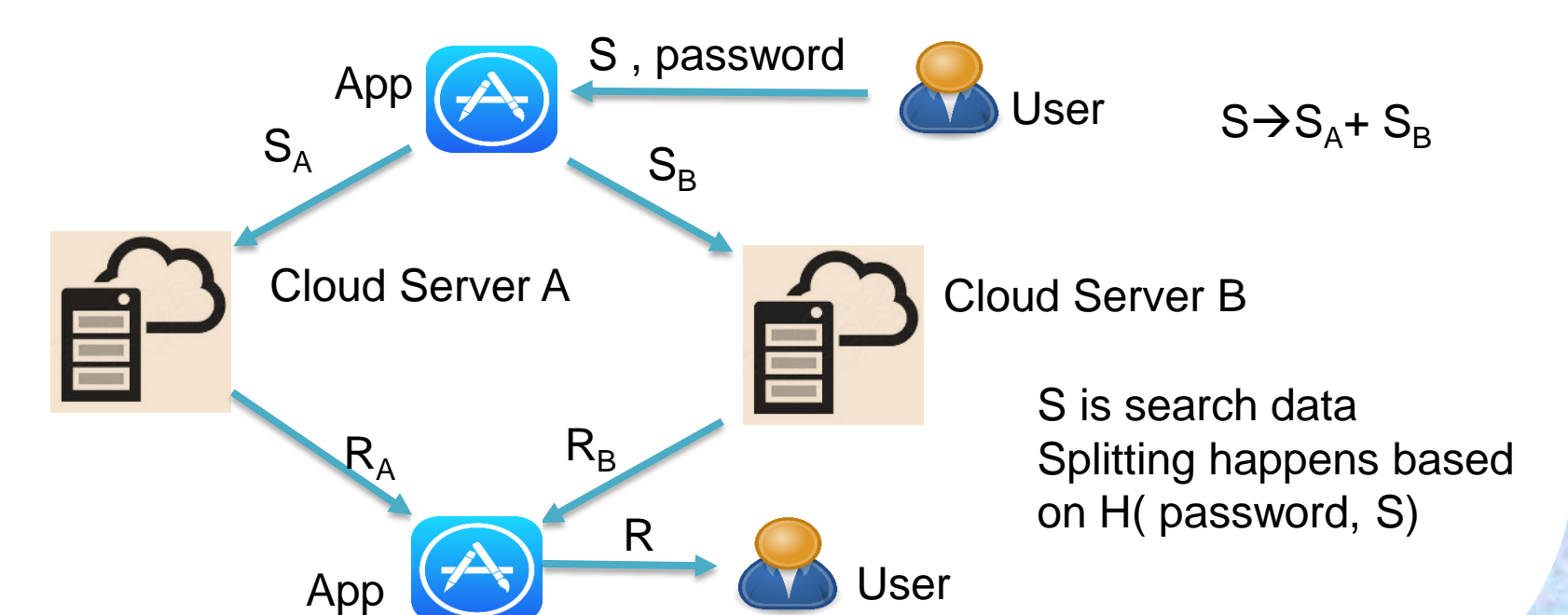
Secure Storage Database

- Data is stored in split form in cloud servers
- Cloud server can't know the data

Storage



Search



Advantages

- **Purpose control** → Misuse of data is prevented
- **No need of Trusted Third Party** → Less expensive
- **Less prone to hacking** → Lower insurance costs
- **Computationally lightweight** → Conserves battery power

Scalability

Basic Arithmetic AS based Computations

- Addition and Subtraction (ASP)
- Multiplication (MP) and Division (DP)
- Exponentiation (EP)
- Greater than Zero (GT0)
- Equivalence with Zero (EW0)

Higher Level Protocols

- Vector Inner Product (VIP)
- Matrix Multiplication (MM)
- Matrix Inverse
- Numerical Methods (Newton's method)
- LU Factorization

Future Work

- Applications
 - Algorithm protection
 - Engineering design
 - Rating schemes in sharing economy platforms
- Additional security features
 - Integrity verification
 - Attack models
 - Access control

Acknowledgements

- NSF CPS Grant # 1329979

References

- Wang, S., Bhandari, S., Atallah, M., Panchal, J.H., Ramani, K., 2014, "Secure Collaborations in Engineering System Design," 2014 ASME International Design Engineering Technical Conferences (I-DETC) and Computers and Information in Engineering (CIE) Conference, August 16-20, 2014, Buffalo, NY, USA.
- Bogetoft P, Christensen DL, Damgård I, Geisler M, Jakobsen T, Krøigaard M, Nielsen JD, Nielsen JB, Nielsen K, Pagter J, Schwartzbach M. Secure multiparty computation goes live. In: Financial Cryptography and Data Security 2009 Feb 23 (pp. 325-343). Springer Berlin Heidelberg.

Advantages

Issues

All the servers conspire to share the data

Benefits

Cloud Server are unaware of each other

Easy updating and data recovery

No single key for encryption which can be hacked

Safe even company or employee wants to get data