CERIAS

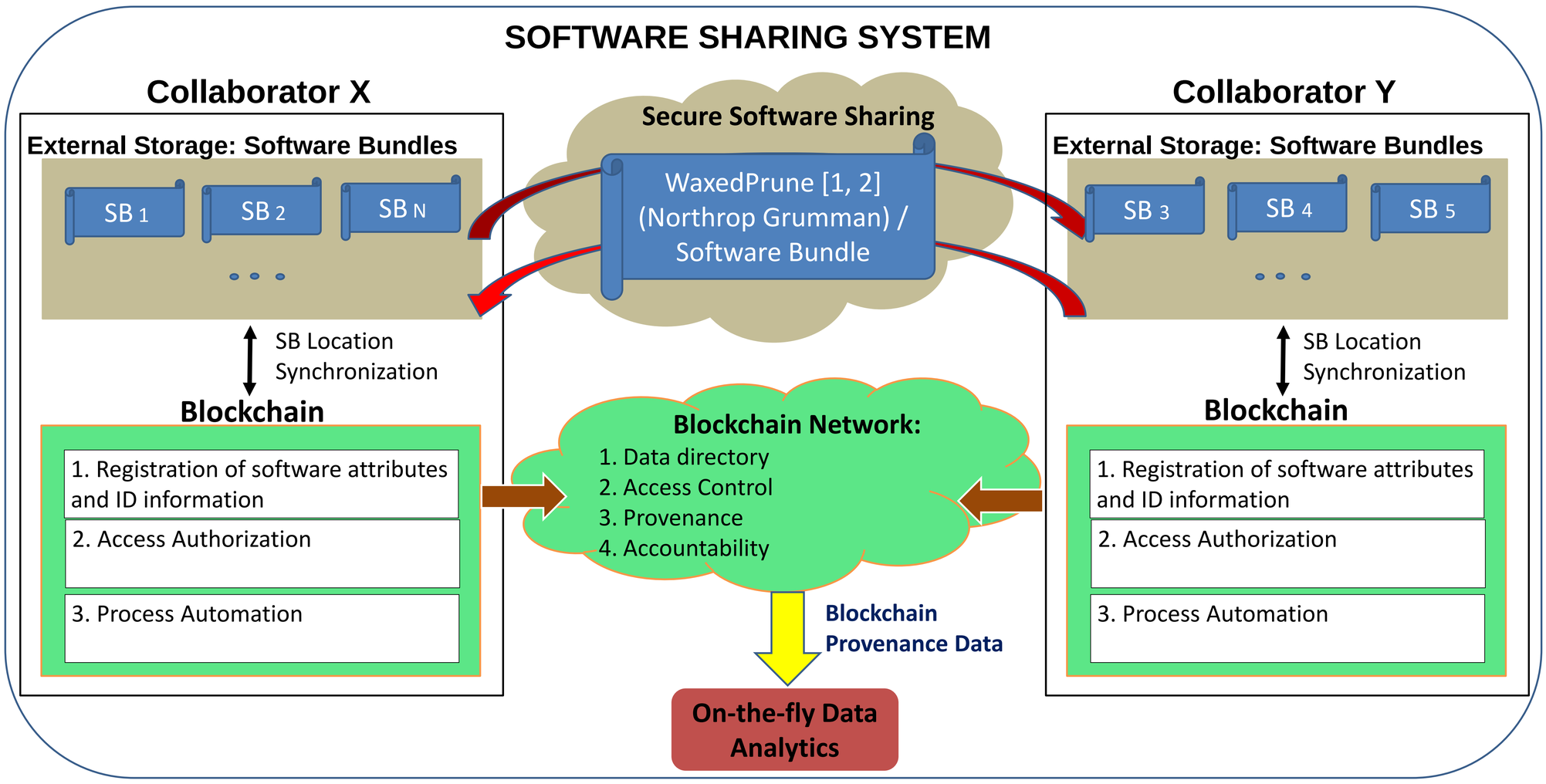
The Center for Education and Research in Information Assurance and Security

Blockhub: Blockchain-based Secure Cross-domain Software Development System

Denis Ulybyshev[1], Bharat Bhargava[1], Miguel Villarreal-Vasquez[1], Aala Alsalem[1], Ganapathy Mani[1], Leszek Lilien[1], Donald Steiner[2], Jason Kobes[2], Steve Seaberg[2], Paul Conoval[2], Robert Pike[2], Rohit Ranchal[3]

[1]Computer Science and CERIAS, Purdue University; [2]Northrop Grumman; [3]IBM

SOFTWARE SHARING SYSTEM



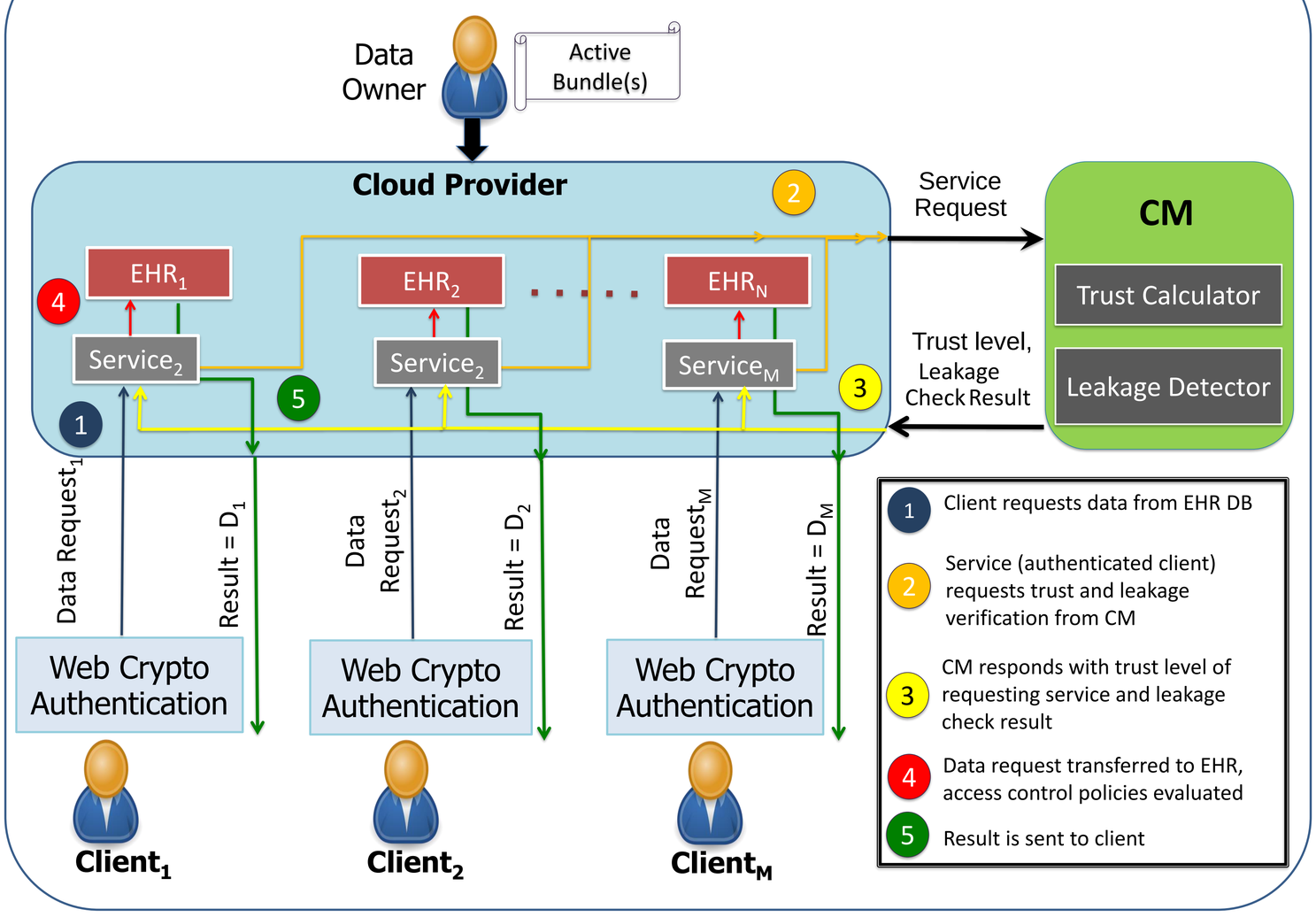
OBJECTIVES

- Provide secure software sharing and software access auditing
- Provide integrity of provenance data
- Detect software spillage

FEATURES

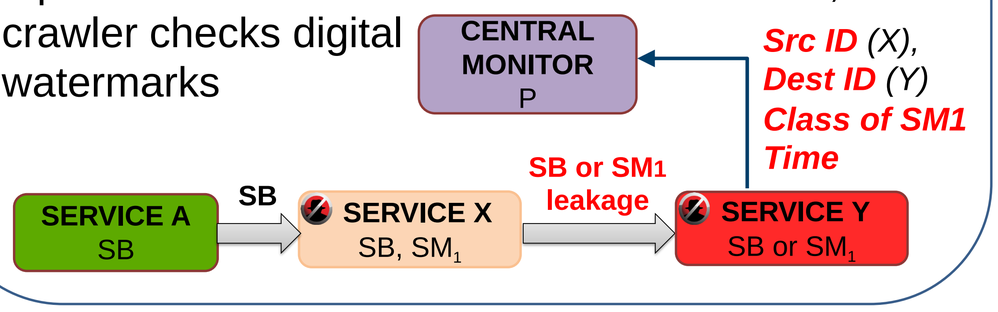
- Encrypted SM is stored in SB
- Role- and attribute-based access control
- X and Y, can share software via smart contracts running in blockchain network
- Every request and transfer of SM is logged in blockchain's distributed ledger
- For software transfer authorization needed by both smart contract and policy enforcement engine of the SB

WAXEDPRUNE ARCHITECTURE



SOFTWARE SPILLAGE DETECTION

- SB contains ***Enc [Software (S)] = {Enc$_{k1}$ (SM$_1$), … , Enc$_{kn}$ (SM$_n$) }*** and Access Control Policies ***(P) = {p$_1$,.., p$_k$}***
- X is authorized to extract and decrypt SM1 from SB
- X leaks Enc(SM1) or SM1 to unauthorized service Y
- When Y tries to decrypt SM1 CM checks policies: whether SM1 is supposed to be at Y
- If plaintext SM1 is leaked: visual watermarks; web crawler checks digital watermarks

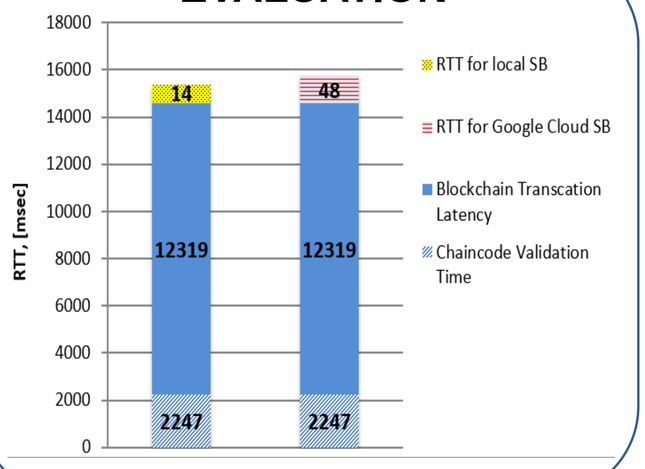


PUBLICATIONS, PROTOTYPE

[1] D. Ulybyshev, B. Bhargava, M. Villarreal-Vasquez, D. Steiner, L. Li, J. Kobes, H. Halpin, R. Ranchal, A. Alsalem, "Privacy-preserving Data Dissemination in Untrusted Cloud", IEEE Cloud 2017

[2] NG WAXEDPRUNE Prototype https://github.com/Denis-Ulybysh/absoa17

EVALUATION



ACKNOWLEDGEMENT: This research is supported by Northrop Grumman. We collaborated with Donald Steiner, Leon Li, Jason Kobes, Steve Seaberg, Peter Meloy, Paul Conoval

PURDUE UNIVERSITY Discovery Park

CERIAS