IEEE Symposium on Security and Privacy
(Short-talks Group-2 IEEE SP 2020)

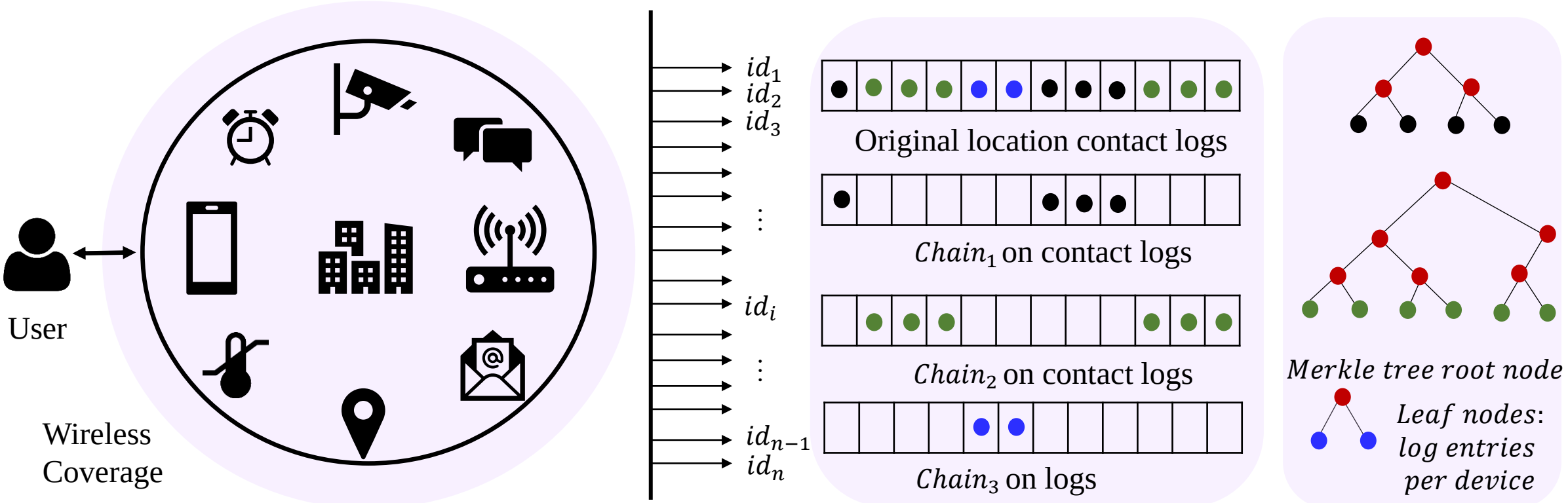
Nisha Panwar
Augusta University
(npanwar@augusta.edu)

Privacy Preserving Model for Contact Tracing Logs

Keywords: localization, privacy, integrity, confidentiality

Contact Tracing Checklist

- Pre-pandemic privacy for contact tracing logs → permission-based
  - *Can user conditionally grant access to the contact tracing data?*
- During pandemic most recent traces have → highest entropy
  - *Can health service providers and virus containment monitoring services have access to most recent traces?*
- Tunable privacy revealing window → delay the permission-based access
  - *Can we leverage a time-released access that would eventually transition into fully permission-based access?*
- The minimal access to trace logs should be enough to elevate and isolate those at high-risk



❶ $Log\ entry < Stream_{id}, Chain_{id}, SN, t, payload >$

❷ $Merkle\ node \rightarrow H(left_{child} || right_{child})$

❸ $Access\ policy \rightarrow Chain_1 = E_{SK_1}(LSN_{11}LSN_{12}LSN_{13} \ldots LSN_{1i})$

❹ $Access\ policy \rightarrow Chain_2 = E_{shared_{key}}(LSN_{21}LSN_{22}LSN_{23} \ldots LSN2_i)$

❺ $Access\ policy \rightarrow Chain_3 = E_{PK_3}(LSN_{31}LSN_{32}LSN_{33} \ldots LSN_{3i})$

❻ $Access\ policy \rightarrow Chain_j = E_{escrow\_key}(LSN_{j1}LSN_{j2}LSN_{j3} \ldots LSN_{ji})$

❶ For log storage

❷ For log integrity verification

❸ PKI based access policy

❹ Authenticated key exchange access policy

❺ Proxy key encryption-based access policy

❻ Trusted third party access policy

Least access

Full access

Questions?

Nisha Panwar
Email: npanwar@augusta.edu