AUGUSTA UNIVERSITY
SCHOOL OF COMPUTER AND CYBER SCIENCES

22nd International Symposium on Network Computing and Applications 2024

WiFi Traffic Inspection for Obscured Devices

Maksuda Rabeya
Nisha Panwar

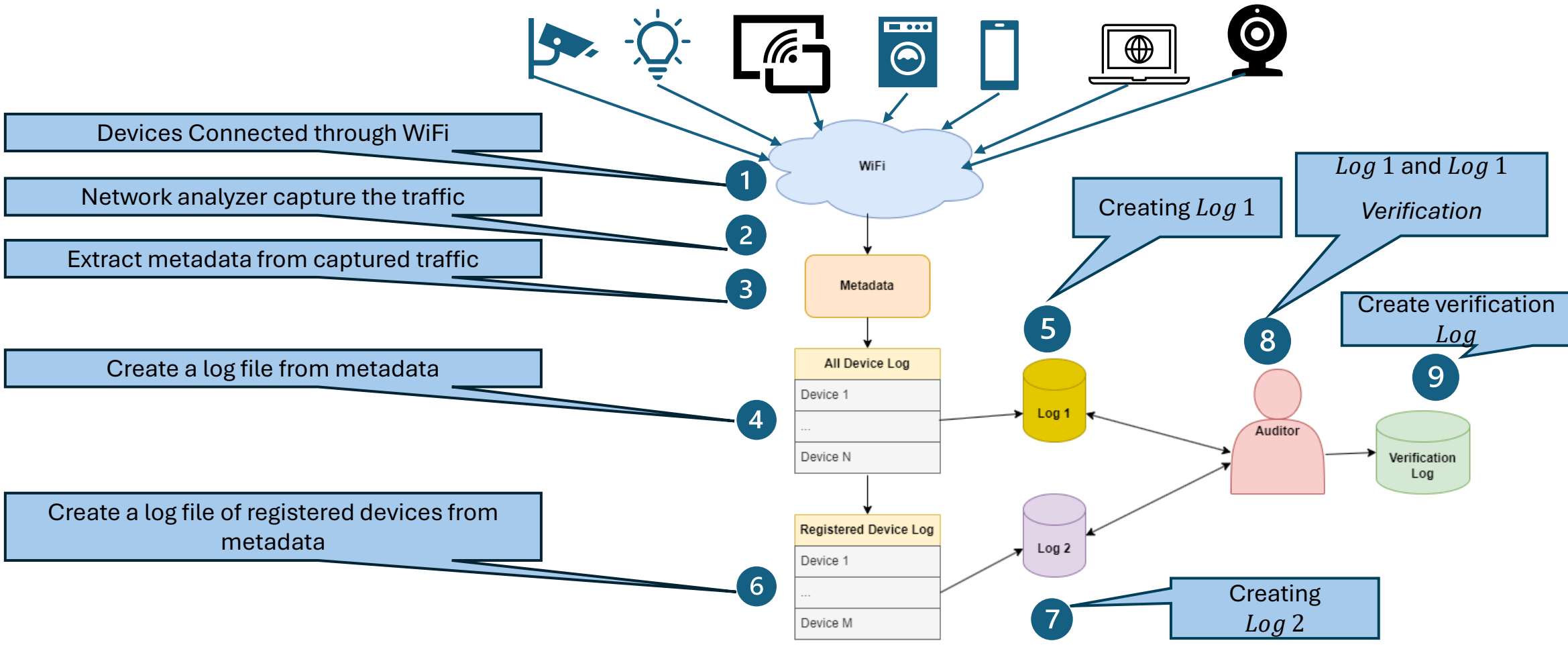
Key Observations

- The IoT communities and sustainable environment calls for security and privacy assurance
- Existing methods provide security solutions but may compromise privacy
  - Auditing includes revealing the metadata in plain text
- Auditing process designed in this work is practical
  - Data structures used in the proposed scheme are memory efficient
  - Guarantee device log integrity through latency saving audit routines
- Captured device logs and current device logs are verifiable
  - MHT based logs leverage efficient auditing for devices that hold credentials
  - Bloom filter based logs leverage efficient auditing for devices that are seen first time on the network.

Security Properties

- Secure WiFi
  - WiFi Protected Access3(WPA3) is the latest standard for secure wireless networks.
  - WiFi employs Advanced Encryption Standard (AES0) for encrypting data during transmission
  - Strong and unique passwords for network access
  - Enabling separate guest network for separate access
- Verifibility
  - Cryptographic hash functions like SHA256 are commonly used to verify integrity
  - Digital Signature is also used to verify the authenticity and integrity of the message
- Privacy
  - Privacy refers to protecting personal or sensitive information as it is transmitted over a network.
  - End-to-end encryption, concealing identity, restriction access, and integrating privacy measures into network architectures and protocol.

Systems Overview



Protocol

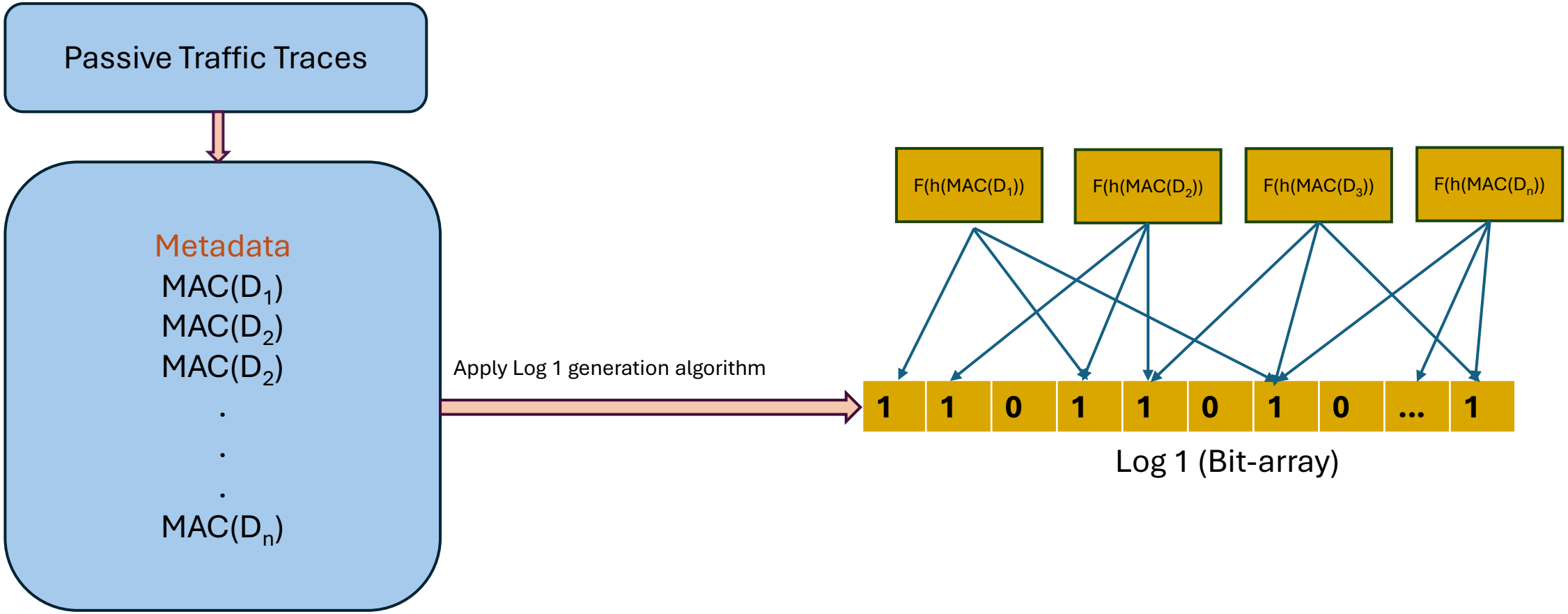
Log 1 Generation

- Collect the metadata from the network traffic.
- Computer the hash function from each device metadata.
- Perform mathematical operations to find the bloom filter index.
- Set the value 1 to the corresponding index of the log.
- After calculating hash, index, and setting 1 to the corresponding index, Finally got the *Log 1*

***The log generation methods do not support updates and deletes

Protocol

Log 1 Generation cont.



***The log generation methods do not support updates and deletes

Protocol

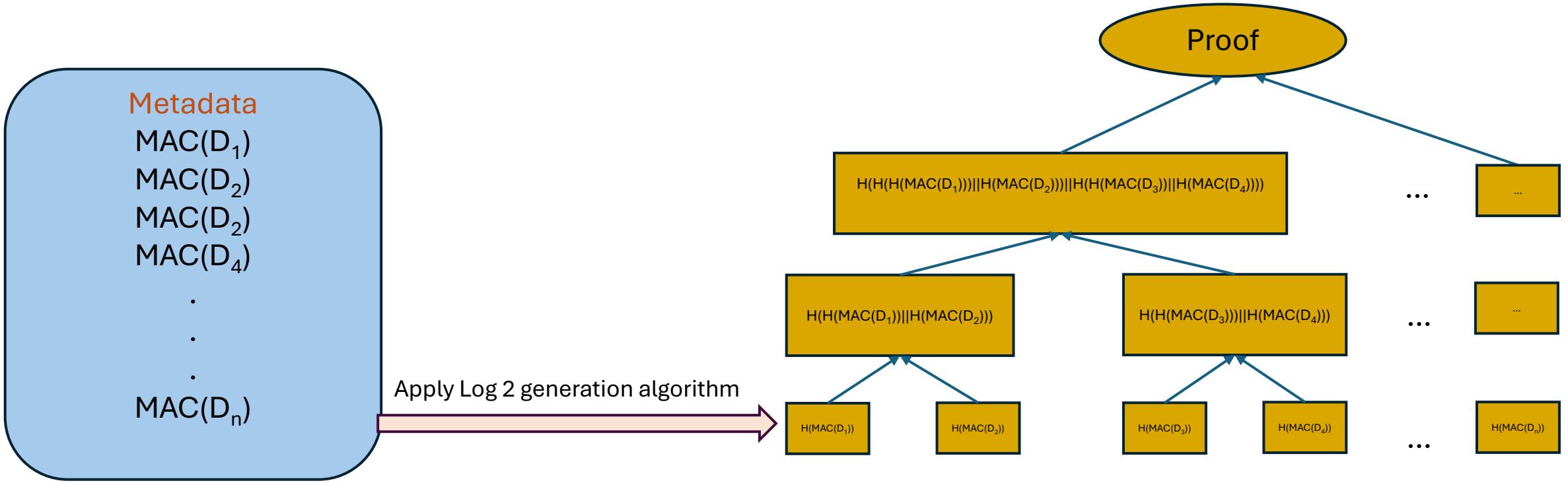
Log 2 Generation

- Collect the metadata from the network traffic.
- Sorted the devices $D_1, D_2, D_3, D_4, \ldots\ldots D_n$
- Compute the hash of each device as a leaf node of the MHT
- Compute the parents from the leaf nodes.
- MHT root is generated from leaf to upward computation of parents.
- Finally, the root node contains the accumulated hash of all devices and generates the *Log 2*

***The log generation methods do not support updates and deletes

Protocol

Log 2 Generation cont.



***The log generation methods do not support updates and deletes

Protocol

Verification of Logs

- Auditor has the *Proof* and *Log1* from the prover.
- *Compare the Log1* with the $Log1_{current}$
- Compared the *MHT_Proof* with the $Log2_{current}$
- If both Comparison shows

  Bit Array == *Log1*

  MHT_Poof == *Log2*

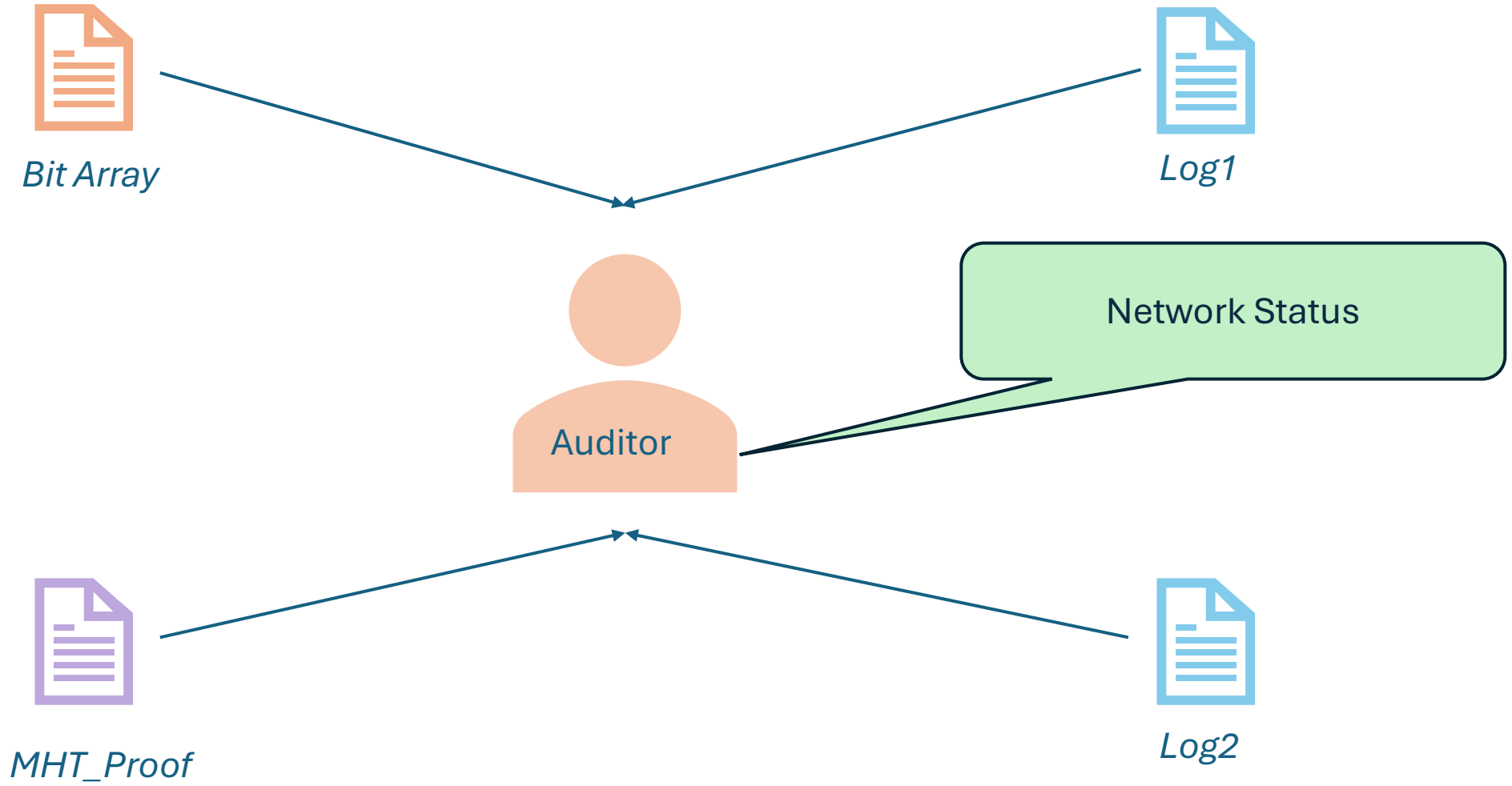
  Then, the verification output =1, which means the network is stable.
- *Else,*

  The verification output =2, which means the network might have compromised

***The log generation methods do not support updates and deletes

Protocol

Verification of Logs cont.



Perform verification operation of logs by the auditor

Experiments

Dataset

- Source: ACI IoT Network Traffic Dataset 2023.
- Network: Computer, Smartphones, Data storage, Sensors, Personal Assistance, and Smart home appliances (Diverse group of devices).
- Data Size: 82.7 GB, We have used 24.3 GB of PCAP files.

Experiments

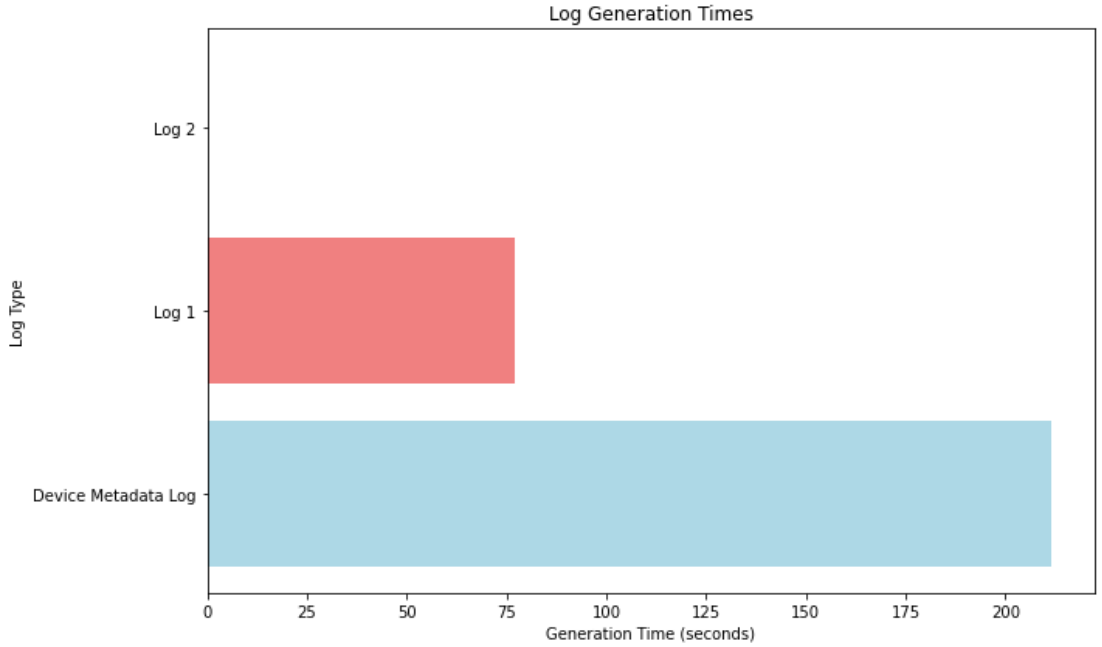
Hardware and Software Environment

PC Configuration	*System Model:* B460MDS3HAC *Manufacturer:* Gigabyte Technology Co. Ltd. *Bios:* F3 *Processor:* Intel(R)Core(TM) i5-10400 CPU@2.90GH *Memory:* 32768 mb
Operating System	Windows 11 Pro 64 bit
Programming Language	Python 3.11
Development Environment	Spyder in Anaconda

Result Analysis

Log Generation Time Comparison

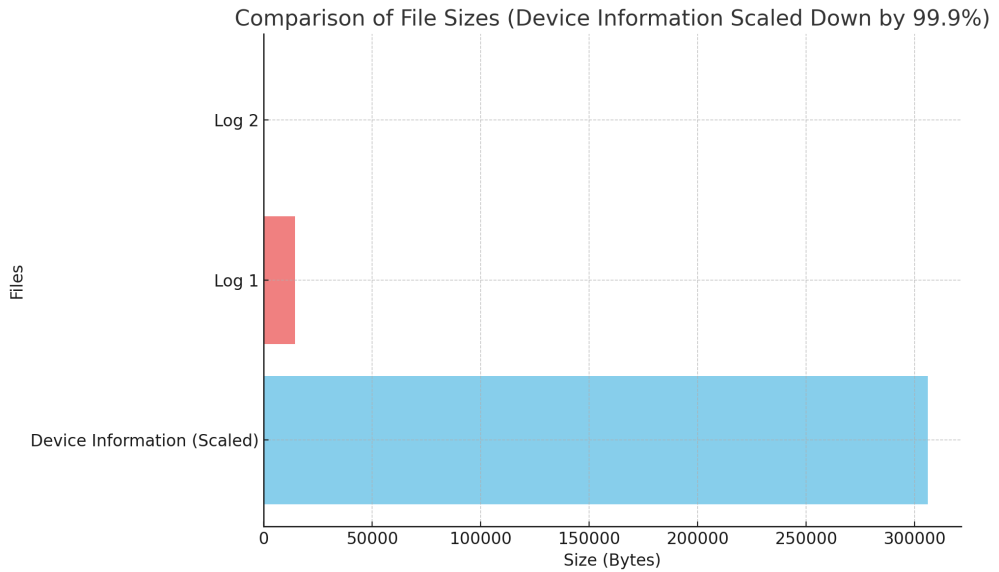
- *Log1* optimized log creation time 62.5%.



Result Analysis

Comparison of Storage Requirement of Different Logs

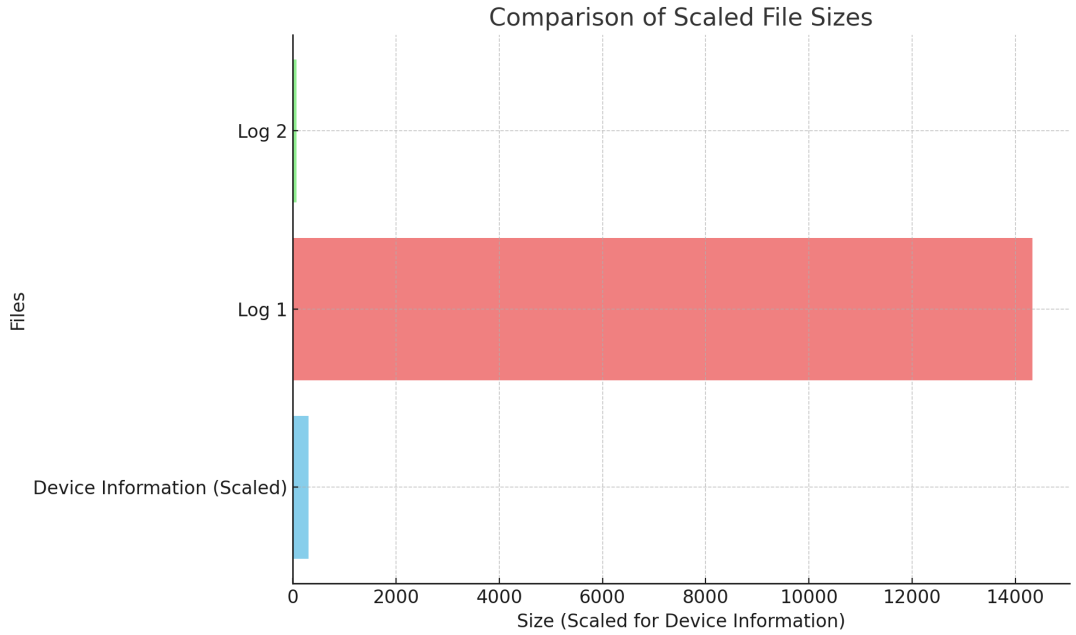
- *Log 1* optimized log creation storage size 14 KB.
- *Log 2* occupies 66 bytes of storage.
- Metadata log occupies 292 MB of storage.



Result Analysis

Comparison of Storage Requirement of Different Logs (Device Scaled Down)

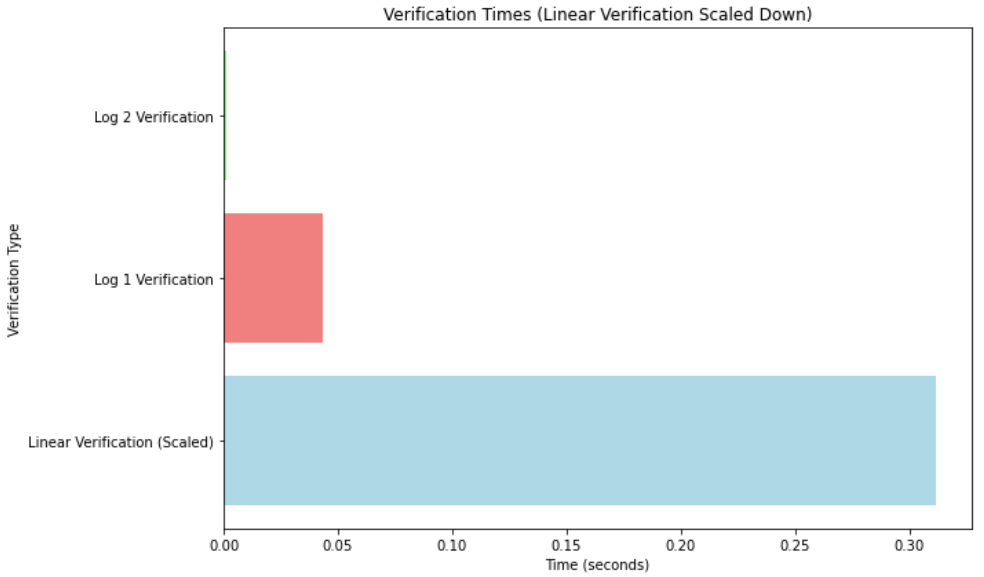
- Although the device log created from metadata is scaled down, still requires 1.63 KB storage for *Log1* since the fixed size Bit-Array.



Result Analysis

Comparison of Verification Time

- *Log1* Verification time is 0.043520 seconds.
- *Log2* Verification time is 0.000969 seconds.
- Metadata log verification requires 31.159 seconds.



Related Work

Research Papers	Key Findings/Contributions
M. Adam et al.(2024), M. Laner et al. (2023), A.Sivanathan et al.(2018), H. Fu et al.(2022), S. Xiong et al. (2022)	•IoT devices provide huge facilities that can be compromised with security. •Different types of IoT devices like M2M and H2M communications •Provide huge traffic flows and required traffic shaping
A.D. Singh et al.(2021), S. Sami et al. (2021), Z.B. Tariq et al.(2017), S.Sami et al. (2021), T. Liu et al. (2018), K. Wu et al. (2019), K. Cheng et al. (2019)	•Different localization techniques, like non-gps •Hidden device detections using smartphone •Detection of spy cameras •Detection of eavesdropping using home appliances and detection using Lidar sensors •Non-registered device detection using RF detectors
S. Sing et al. (2009)	•Network auditing involves assessing the security architecture, policies, and procedures of an organization. •Network users and systems involved in the audit process should be authenticated using multifactor authentication. •Cryptographic techniques like hashing and digital signatures should be used for integrity.
T. Taassori et al. (2018), A.Miller et al. (2014), M.S. Niaz et al. (2015), J. Hieb et al. (2012)	•Authenticated data structures and how they preserve the integrity •Ensuring data verification, data security, access control, non-repudiation, and compliance with regulation.

Important Takeaway

- The proposed solution ensures privacy-preserving verification of WiFi traffic.
- The privacy-first approach guarantees *minimal storage* and maintenance of device metadata logs.
- Enhances the verification latency through derivative proofs accumulated through Bloom filter-based log generation.
- The proposed scheme is practical, and implementation is feasible.
- In the future more advanced data structures are focused to optimize the performance of the proposed algorithms.
- The progressive increase in device connections must adapt the latency of verification.

Thank You

Questions

Email: mrabeya@augusta.edu