Lightweight Mutual Authentication for Inter Cloud Services Using Edge Computing by Computer Security Chiefs

Donda, Vinay Kumar Reddy (Team Lead)
N V Ravi Kishor Mokkapati
Lakshmi Pravallika Somisetty
Madhav Kilaru
Sarath Boddu
Abhinay Edara

Inter Cloud Services - Abstract

- Insight on redeemable payment protocol and lightweight authentication of IoT devices with cloud servers to avail services
- Using payment tokens, proof of subscription, Merkle Tree, tree of secrets, hash chains
- Four phases are involved
  - Registration & set-up
  - Mutual authentication
  - Message exchange
  - Payment redemption
- Provides authentication, confidentiality, integrity, anonymity to user, resilience to replay attacks, traceability of invalid device

Inter Cloud Services - Introduction

- Cloud – Edge – IoT Architecture
- Computational offloading using edge nodes and cloud servers
- IoT devices – limited storage
- Mutual Authentication needed between edge nodes and IoT devices
- High quality services
- Foreign edge nodes are to be fairly compensated
- IoT devices uses payment tokens and proof of subscription to host cloud servers

Inter Cloud Services

Benefits of this approach

- Storage needed at IoT gateway is reduced
- One way hash chains – CO services provided to fairly compensate foreign edge nodes
- Symmetric key protocol used - using secret key – Tree of secrets and thus storage reduced
- Not an ECC - not suitable to IoT devices
    - discrete logarithm problem
    - more computation needed

Inter Cloud Services

Edge Computing

- Lowest level of cloud execution – edge of the internet
- Placed between IoT devices and cloud servers
- Most of the enterprises using this

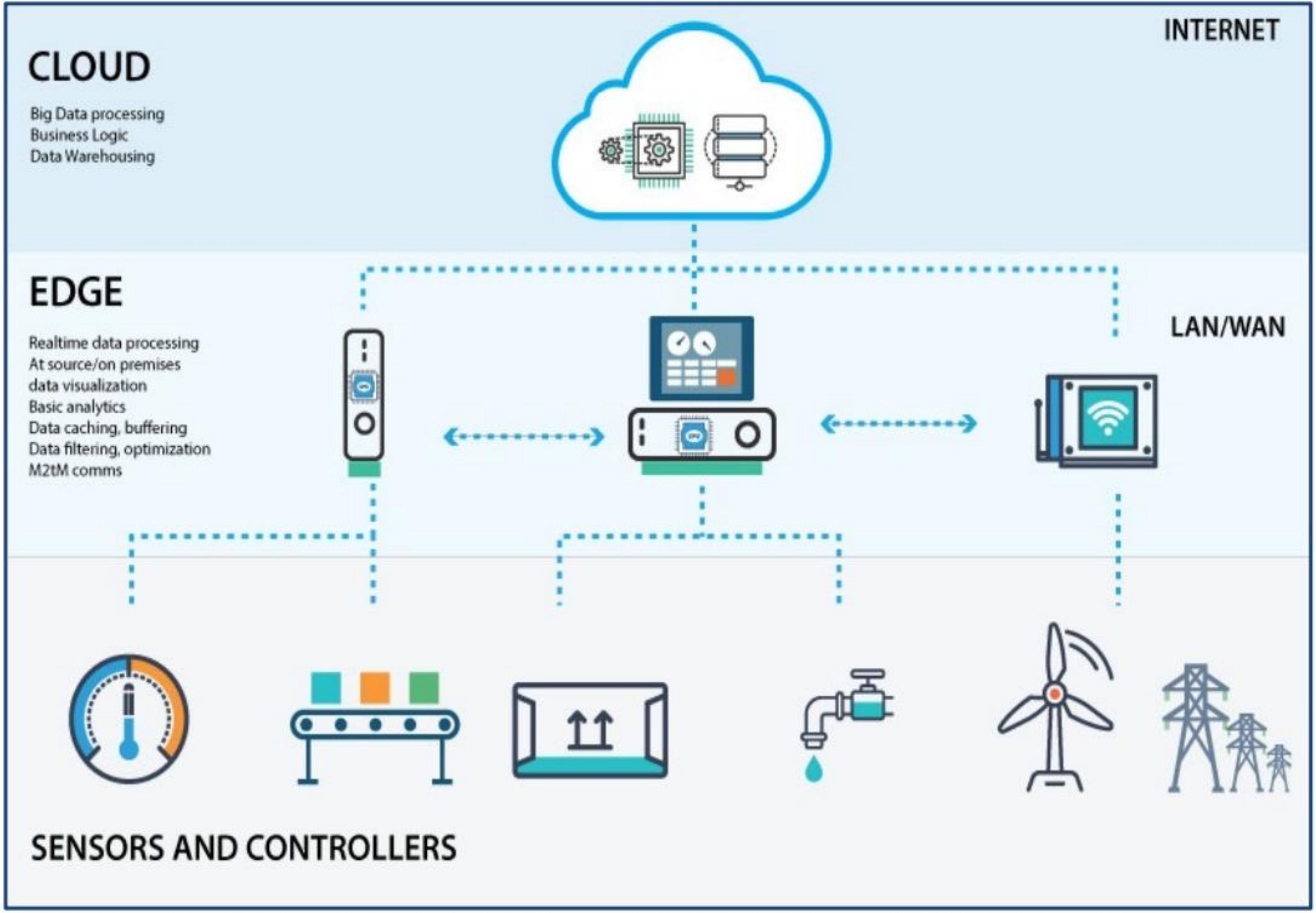
Drivers behind Edge Computing

- Connectivity – continued service
- Latency – low Round Trip Time
- Bandwidth – Communication optimization from Cloud
- Privacy/Security – Data not stored on cloud

AWS Lamba functions – less code, more functionality

- `test = lambda x : True if (x > 10 and x < 20) else False`

Inter Cloud Services



INTERNET

CLOUD

Big Data processing
Business Logic
Data Warehousing

EDGE

Realtime data processing
At source/on premises
data visualization
Basic analytics
Data caching, buffering
Data filtering, optimization
M2tM comms

LAN/WAN

SENSORS AND CONTROLLERS

Inter Cloud Services

Edge Computing used in below areas

- Public safety, health and education, military
- Smart farming and smart parking

Advantages of Edge Computing

- Pre-process, pre-fetch, filter unwanted data
- Reduce bandwidth, load, latency
- Data Caching
    - performance
    - offline tasks
    - resource efficiency

Inter Cloud Services

IoT devices – Network of interconnected devices

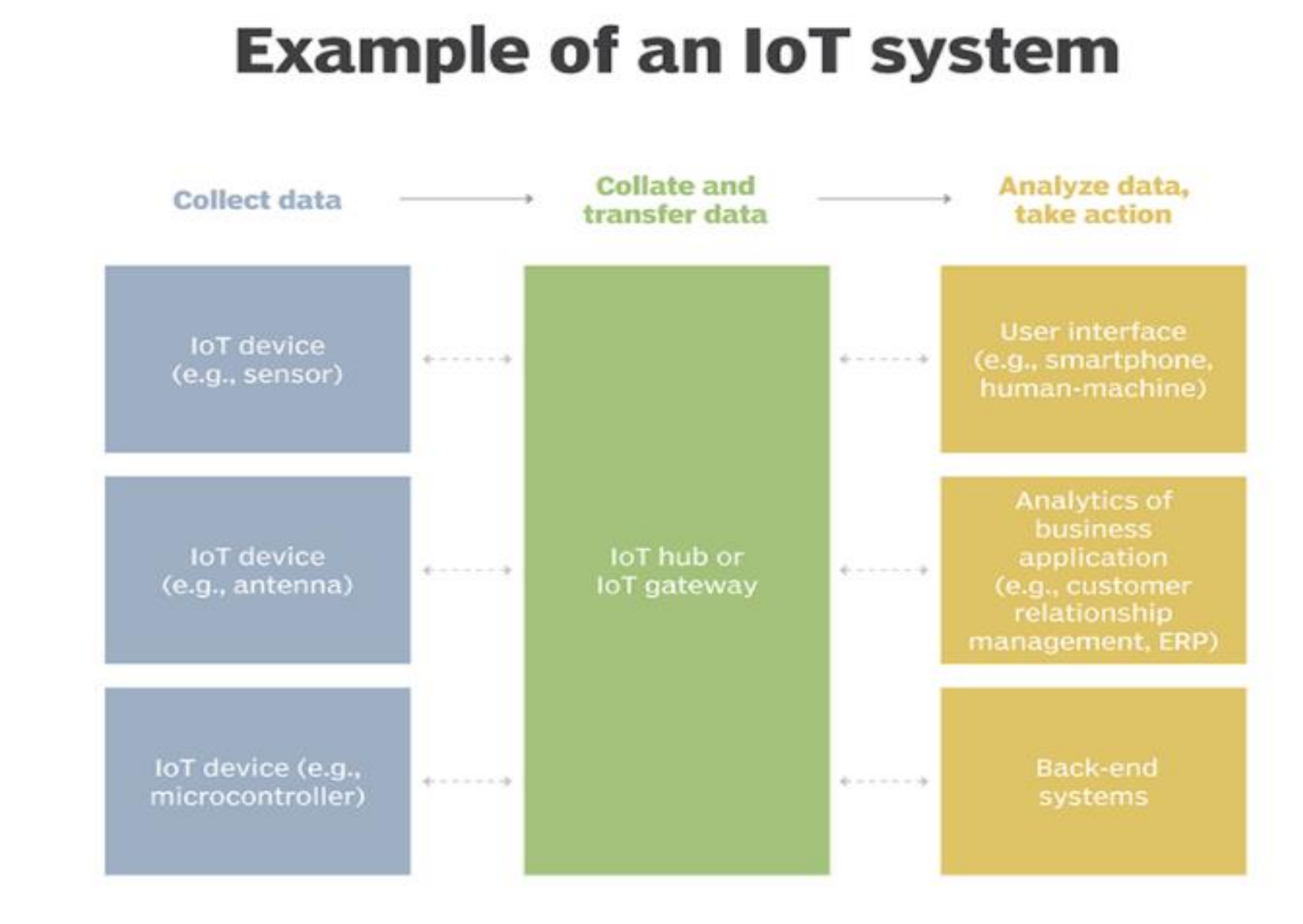
- Machines
- Devices
- Objects
- Animals or humans with unique identifiers (UIDs)

Architecture

- Lightweight communication software
- Lightweight hardware
- Sensors and CPUs

IoT devices communicate with each other using blockchain but can be controlled by humans

Inter Cloud Services



Example of an IoT system

Collect data
Collate and transfer data
Analyze data, take action
IoT device (e.g., sensor)
IoT device (e.g., antenna)
IoT device (e.g., microcontroller)
IoT hub or IoT gateway
User interface (e.g., smartphone, human-machine)
Analytics of business application (e.g., customer relationship management, ERP)
Back-end systems

Inter Cloud Services

IoT Devices

- Home automation – Alexa devices, lights, fans, thermostats
- Wearable Devices – Watches, headsets
- Sensors – construction traffic
- Medical surgical instruments
- Agriculture equipment smart devices

Inter Cloud Services

IoT Devices

Pros:

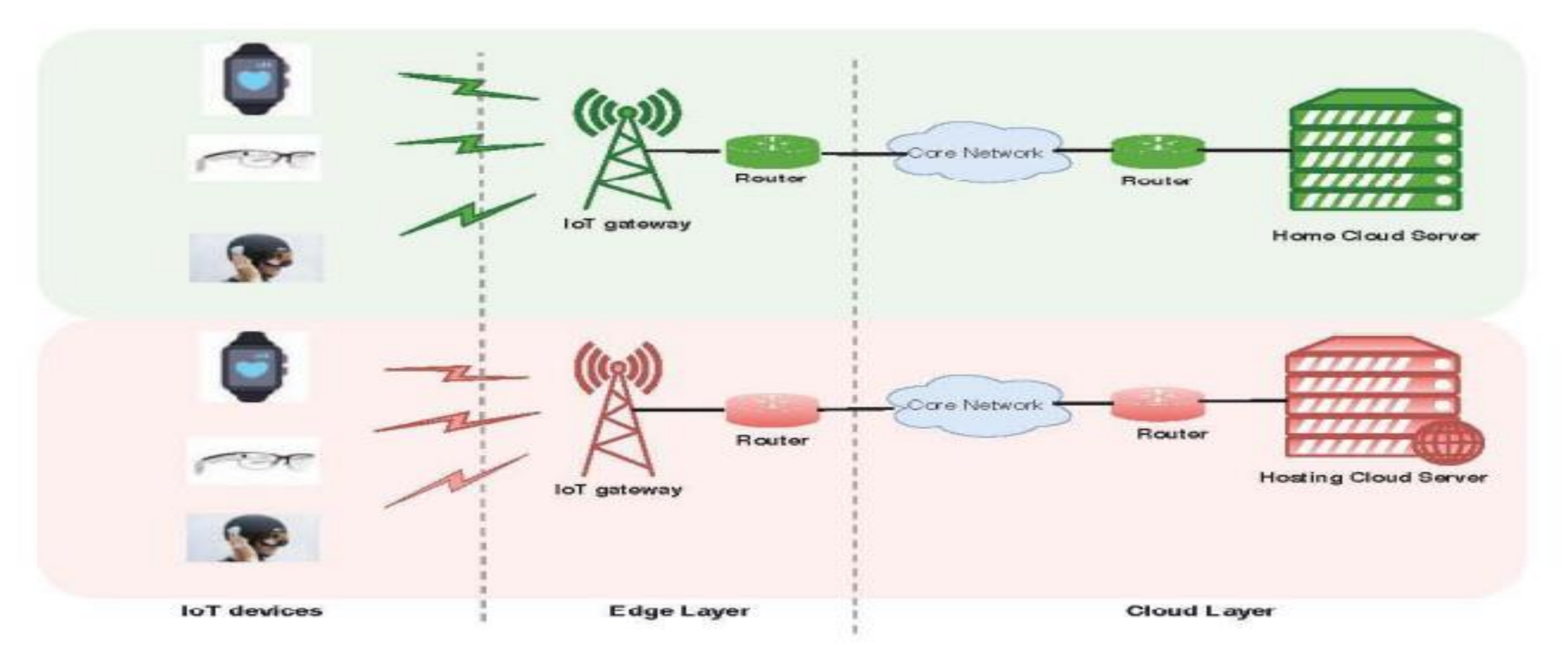
- Access services thru internet – any time, anywhere
- Improved connection – less time and effort
- Automation – less human intervention & more quality

Cons:

- Number of device increases – less confidentiality because of leakage
- Huge data – difficult to manage
- One defect – entire system vulnerable
- No common framework with different vendors. WIP progress on this part by international organizations

Inter Cloud Services

- System Model
  - Cloud Admins deployed by cloud service providers – registration, subscription
  - IoT Gateways – storage & computation power
  - IoT Devices – resource constrained devices



Inter Cloud Services

Threat Model

- A trusted and secure CA is needed
- A trusted and secure IoT gateway securely connected to a CA
- Malicious IoT device trying to get CO services without proof of subscription
- Denial of service over the IoT gateway

Inter Cloud Services

Design goals

- Mutual authentication between IoT device and host cloud’s IoT gateway
- Integrity and confidentiality between messages exchanged
- Tracking the misbehaved IoT device by identifying its real identity
- Avoiding public key cryptography and using symmetric key cryptography
- Guaranteed payment to IoT gateway of the host cloud server for the CO services provided.

Inter Cloud Services

Protocol Design and Implementation

- IoT device moves out of home cloud’s (CAh) network area
- It should be in the range of host cloud’s (CAv) gateway serving areas
- IoT device (IoTh) authenticates itself with CAv by providing
    - payment tokens and subscription proof from CAh
- CAv validates subscription evidence and confirms the payment token for the CO services provided to IoTh
    - using Merkle Trees and Tree of secrets
- CAv gathers tokens from IoT gateway (GAv) and redeem charges from CAh

Inter Cloud Services

Above implementation is achieved using below steps

- 1. Registration & setup phase
- 2. Mutual Authentication phase
- 3. Message Exchange
- 4. Computation charges redemption

Acronyms

- CAh – Home cloud
- CAv – Host cloud(foreign or external)
- IoTh – IoT device
- GAv – Gateway of host cloud

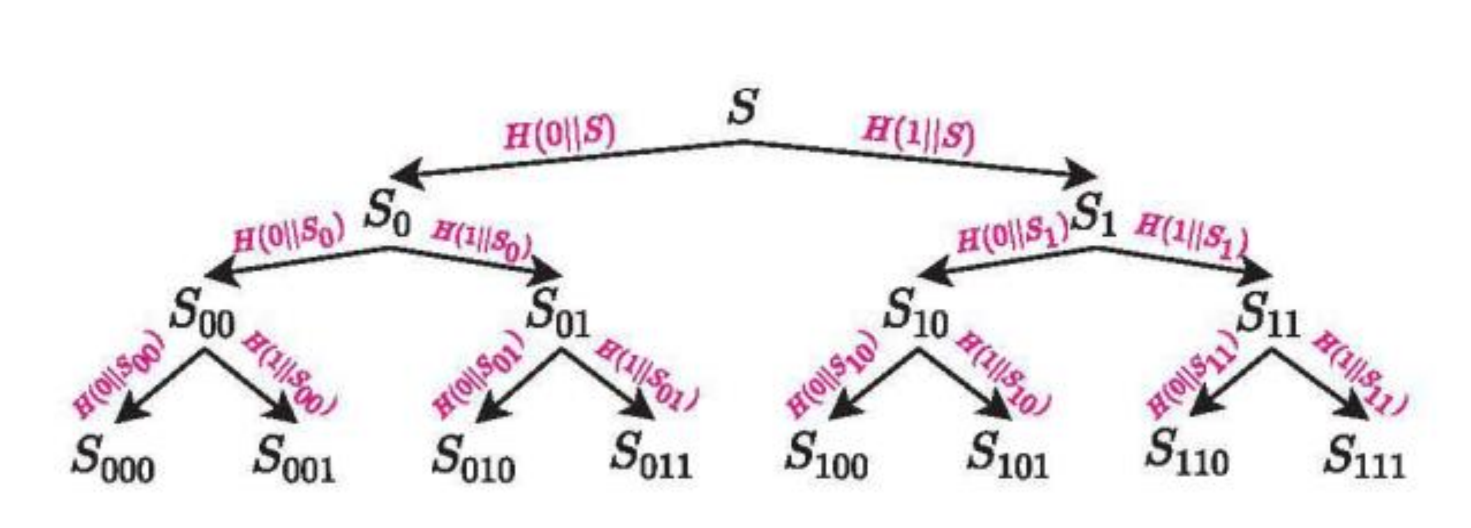
Inter Cloud Services

1. Registration & setup

- CAh setups two keys

  - K known only to CAh & S – to generate Tree of secrets for each and every IoTh

- CAh sends set of secrets to CAv when needed, pseudo identities used to authenticate to Gav (Credit, Aadhar)
- For IoTh index i = 010, S0,S01,S010 are the set of secrets



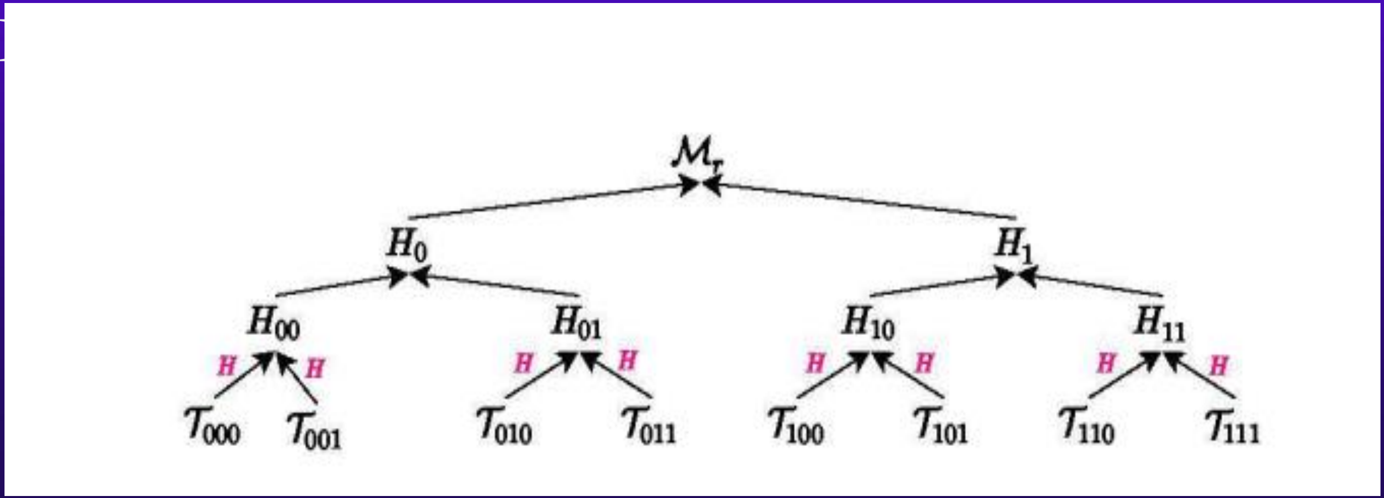
Inter Cloud Services

- CAh constructs hash chain with seed value (Ci) & Merkle tip (Ti) of the hash chain

  - Ci = H (K || Si), here i = 010 as considered previously

  - Ti = H^L(Ci)

- CAh constructs Merkle Tree with all the tip (Ti) values
- For each IoTh, CAh send CAv - Ci, Ti, secrets(S0,S01,S010) and Πi
- Πi is the Merkle proof associated with the tip Ti in CAh



Inter Cloud Services

- For IoT010, secrets are S0,S01,S010 and Merkle path is Π010 = [H(T010), H01, H0]

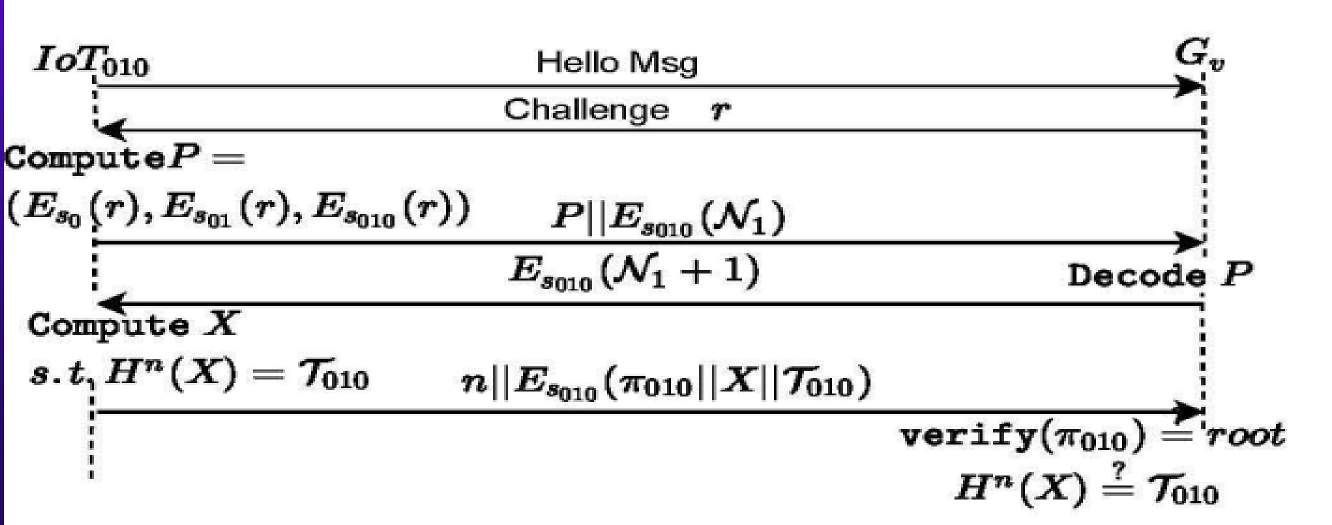
CAh to CAv – home cloud to host cloud

- Sends secret key S and Merkle root Mr
- CAv uses the secret key S to decode temporary pseudo IDs of IoT devices for mutual authentication
- Mr is used to verify the Merkle proof of the IoT tip Ti

Inter Cloud Services

2. Mutual Authentication Phase

- IoT010 sends ‘Hello’ to Gav, Gav challenges IoT010 with r
- IoT010 sends P – pseudo ID as E(s0(r)),E(s01(r)),E(s010(r))
- In addition, IoT010 challenges Gav with nonce N1
- GAv decodes pseudo IDs using traversing from root to using the above encryption path.
- GAv once validates & authenticates IoT010, then sends encrypted N1+1 using s010

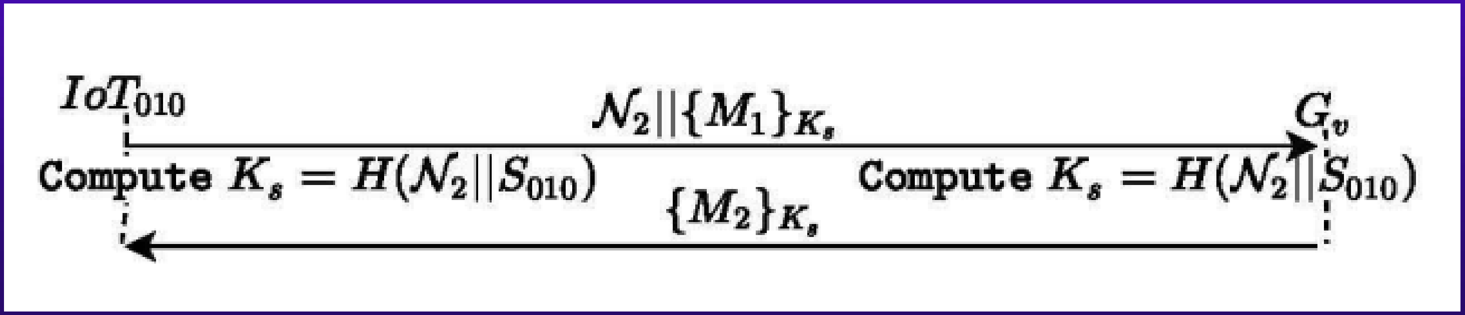


IoT_{010}
Hello Msg
G_v
Challenge r
Compute$P =$
$(E_{s_0}(r), E_{s_{01}}(r), E_{s_{010}}(r))$
$P||E_{s_{010}}(\mathcal{N}_1)$
$E_{s_{010}}(\mathcal{N}_1 + 1)$
Decode P
Compute X
$s.t, H^n(X) = \mathcal{T}_{010}$
$n||E_{s_{010}}(\pi_{010}||X||\mathcal{T}_{010})$
verify$(\pi_{010}) = root$
$H^n(X) \overset{?}{=} \mathcal{T}_{010}$

Inter Cloud Services

3. Message Exchange Phase

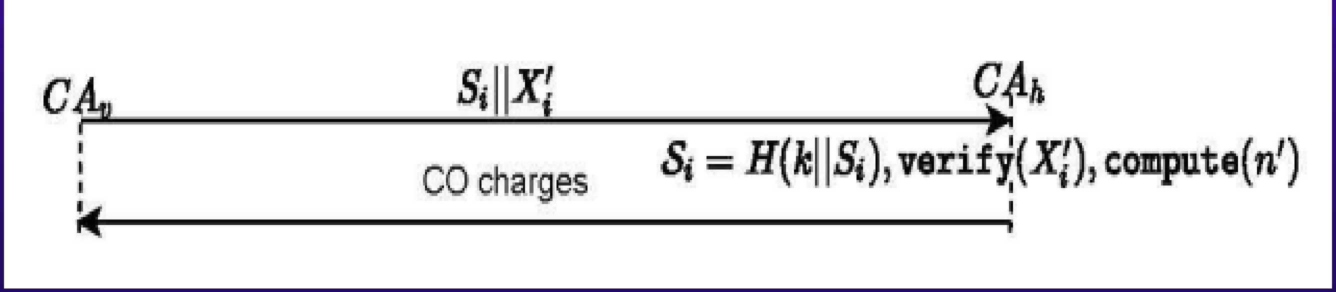
- By using Nonce N2, IoT010 and GAv derives session key Ks = H(N2||S010)
- Ks is used for encrypted message exchange
- M1 & M2 are messages exchanged using Ks


IoT_{010}
$N_2||\{M_1\}_{K_s}$
G_v
Compute $K_s = H(N_2||S_{010})$
$\{M_2\}_{K_s}$
Compute $K_s = H(N_2||S_{010})$

Inter Cloud Services

4. CO Charges Redemption Phase

- CAv sends pseudo identities of IoTh and payment tokens X1 to CAh
- CAh initiates counter as 0 and hashes the seed value Ci until it is equal to the payment token X1
- If c=L, length of hash chain without matching to X1, then it is an invalid token
- Else, CAh pays back CAv for CO units as n = L - c


CA_v
$S_i||X'_i$
CA_h
$S_i = H(k||S_i), \texttt{verify}(X'_i), \texttt{compute}(n')$
CO charges

Inter Cloud Services

Security Analysis

1) Mutual Authentication

- P – Tree of secrets is used to authenticate IoT devices to host cloud-IoT gateway.
- It is minimal that IoTh being identified as IoTh1
- IoTh authenticates IoT gateway using Nonce N1, decodes pseudo identity of IoT device using P and sends encrypted response as N1+1 using secret Si assigned to IoT device.

2) Confidentiality & Integrity

- These are achieved using mechanism mentioned as per the previous step

Inter Cloud Services

3) Guaranteed token redemption

- Pre-image value in the form of payment tokens using hash chains is provided by IoTh to CAv
- Merkle proof tip value is provided only by valid IoT device which is validated as H^n(X) = T; n- computational units and X – payment token
- CAh pays back for n CO units to CAv
- CAh compute Ci = H(K||Si) and verifies payment token in the hash chain
- As K is known only to CAh, probability that IoT gateway identifying X1 as H^n1(X1) = T is negligible

Ti = H^L(Ci)

Inter Cloud Services

4) Resilience to Replay Attacks

- Using nonces N1,N2 and challenge r, replay attacks are reverted i.e., difficult for someone to intrude

5) Pseudo anonymity of user

- IoTh registers to home cloud using real identity
- CAh generates tree of secrets and hides IoTh’s real identity
- CAv uses pseudo IDs of IoThs
- Privacy and security are provided for IoT devices

Inter Cloud Services

6) Traceability of Invalid device

- If misbehaved or invalid IoTh tries to access CAv, CAv finds and CAh will confirm the same to CAv by using Merkle proof tip values.

Inter Cloud Services

Performance Evaluation

To achieve better performance in this system, we consider nonces, challenge r and secret keys to be 128 bits and below are some of the details

Description	Value
IoT storage	(1 + 2*Log N) * 16 bytes
Gateway storage	2*(Ns + 1) * 16 bytes
IoT computation	(L-n) hash, (3 + Log N) Encryption, 1 Decryption
Gateway computation	(n + 1 + Log N) hash, (1 + 2* Log N) Encryption, 3 Decryption
Communication overhead	117. 32 * Log N bytes

Inter Cloud Services

Conclusion

- Mutual authentication between IoT device and multi cloud providers is discussed
- Storage need by IoT gateway is 32 bits for each IoT device
- Only 128 bit keys are shared by cloud admins to generate pseudo identities and Merkle root for the tips of the hash chain
- Payment provided to hosting cloud provider based on computation offloading services offered to IOT device based on its subscription and accumulation in Merkle tree.

Inter Cloud Services

References

- C. Lin, D. H.-K. (2019). Home chain: a blockchain-based secure mutual authentication system for smart homes.
- Choi, B. Y. (2021). Edge Computing. In *Cloud Computing*.
- H. El-Sayed, S. S.-T. (2017). *Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment*
- M. Nakkar, M. S. (2020). *IEEE Internet of Things Journal*
- F. Wang, Y. X. (2018). *IEEE Internet of Things Journal*, vol. 6, no. 3,pp. 4462-4471
- Z. Li, J. K. (2017). Blockchain for secure energy trading in industrial internet of things. *IEEE transactions on industrial informatics*