Widening IoT Security: 3rd-Party Authentication in Federated Cloud, Edge, and Fog Systems

Student: Asad Ali

Advisor: Prof. Dr. Ying-Dar Lin

High Speed Networks Lab

NCTU, Taiwan

Outline

- Federation Motivation
- Federation Background
  - Cloud-Edge-Fog Architecture
  - Cloud-Edge-Fog Federation Scenarios
  - Federation Classification
  - Protocols based Classification
- Federation Issues
- Federation Survey
- Problem-I: 3rd-Party Authentication in Federated MECs
- Problem-II: 3rd-Party Authentication in Federated Cloud-Edge
- Problem-III: 3rd-Party Authentication
- Problem-IV: 3rd-Party Authentication
- References

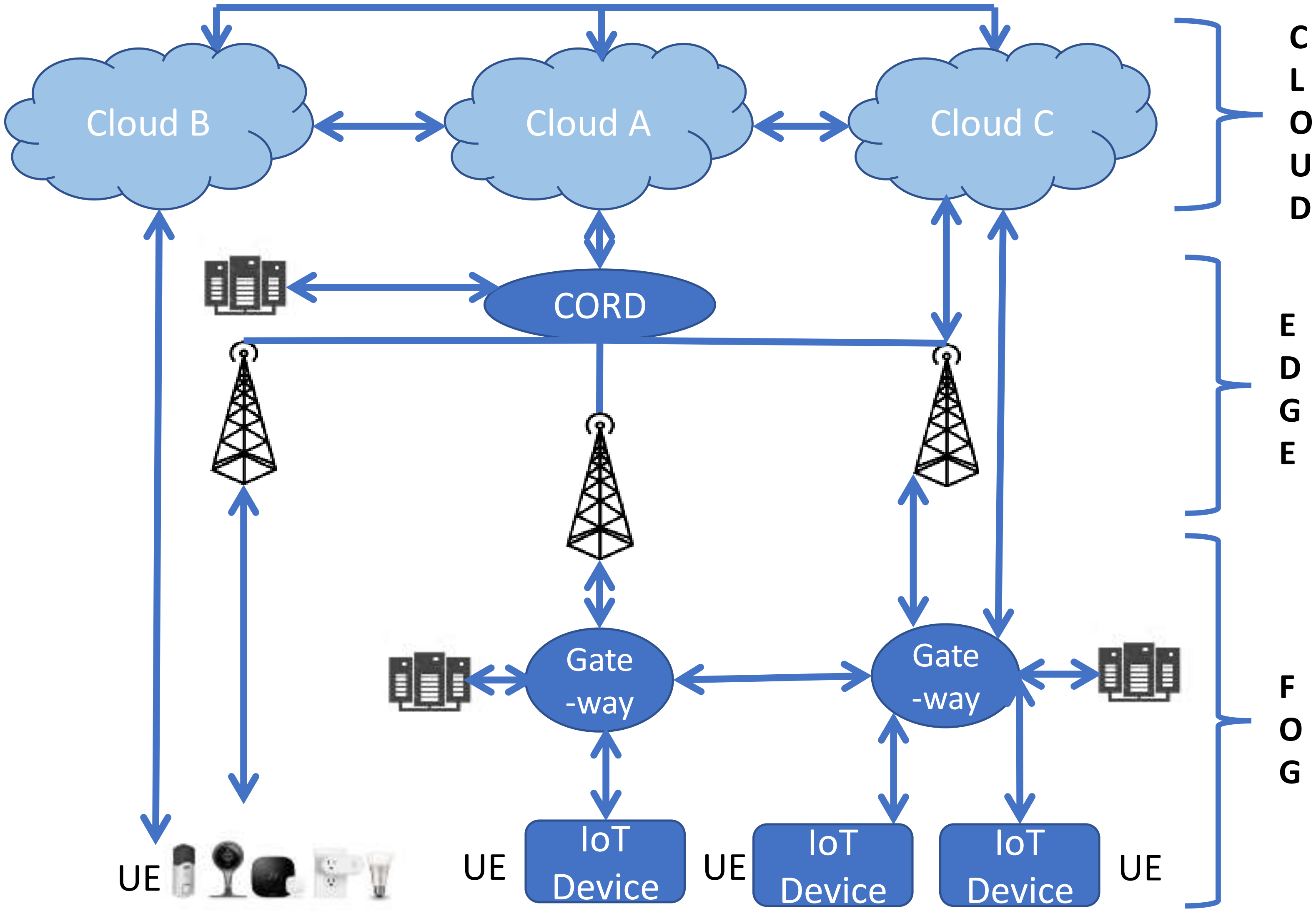
Federation Motivation-I

- Cloud:
  - Far
  - Better Computing Power
  - More Storage
- Fog and Edge:
  - Cloud Near the Ground
  - Geographical Distribution
  - Latency Reduction
  - Bandwidth Savings
  - Better QoS [1]

Federation Motivation-II

- Federation Brings:
  - Optimized Services
  - Enhanced Capabilities for:
    - Data Aggregation
    - Processing
    - Storage
  - Best of all worlds
- Authentication in Federated Cloud/Edge/Fog

Cloud-Edge-Fog Architecture



Federation Scenarios-I

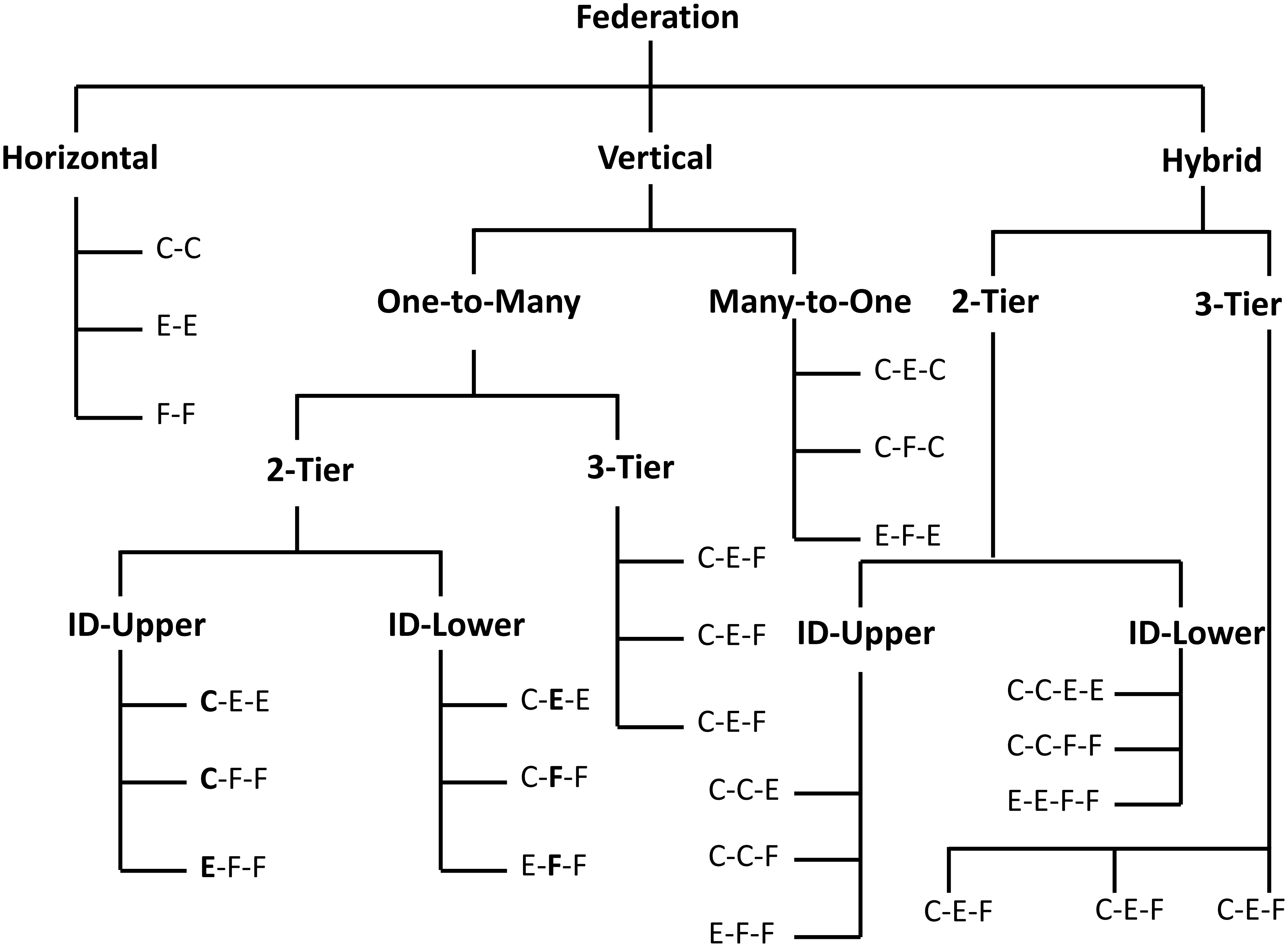
Scenario	Federation	Category	ID Location
1	Cloud-Cloud	Horizontal	Cloud
2	Edge-Edge	Horizontal	Edge
3	Fog-Fog	Horizontal	Fog
4	Cloud-Edge-Edge	2-Tier one-to-many Vertical-ID upper tier	Cloud
5	Cloud-Fog-Fog	2-Tier one-to-many Vertical-ID upper tier	Cloud
6	Edge-Fog-Fog	2-Tier one-to-many Vertical-ID upper tier	Edge
7	Cloud-Edge-Edge	2-Tier one-to-many Vertical-ID lower tier	Edge
8	Cloud-Fog-Fog	2-Tier one-to-many Vertical-ID lower tier	Fog
9	Edge-Fog-Fog	2-Tier one-to-many Vertical-ID lower tier	Fog
10	Cloud-Edge-Fog	3-Tier Vertical	Cloud
11	Cloud-Edge-Fog	3-Tier Vertical	Edge
12	Cloud-Edge-Fog	3-Tier Vertical	Fog

Federation Scenarios-II

Scenario	Federation	Categories	ID Location
13	Cloud-Edge-Cloud	2-Tier Many-to-one Vertical	Cloud
14	Edge-Fog-Edge	2-Tier Many-to-one Vertical	Edge
15	Cloud-Fog-Cloud	2-Tier Many-to-one Vertical	Cloud
16	Cloud-Cloud-Edge	2-Tier Hybrid-ID upper tier	Cloud
17	Cloud-Cloud-Fog	2-Tier Hybrid-ID upper tier	Cloud
18	Edge-Edge-Fog	2-Tier Hybrid-ID upper tier	Edge
19	Cloud-Cloud-Edge-Edge	2-Tier Hybrid-ID lower tier	Edge
20	Cloud-Cloud-Fog-Fog	2-Tier Hybrid-ID lower tier	Fog
21	Edge-Edge-Fog-Fog	2-Tier Hybrid-ID lower tier	Fog
22	Cloud-Edge-Fog	3-Tier Hybrid	Cloud
23	Cloud-Edge-Fog	3-Tier Hybrid	Edge
24	Cloud-Edge-Fog	3-Tier Hybrid	Fog

Federation Classification

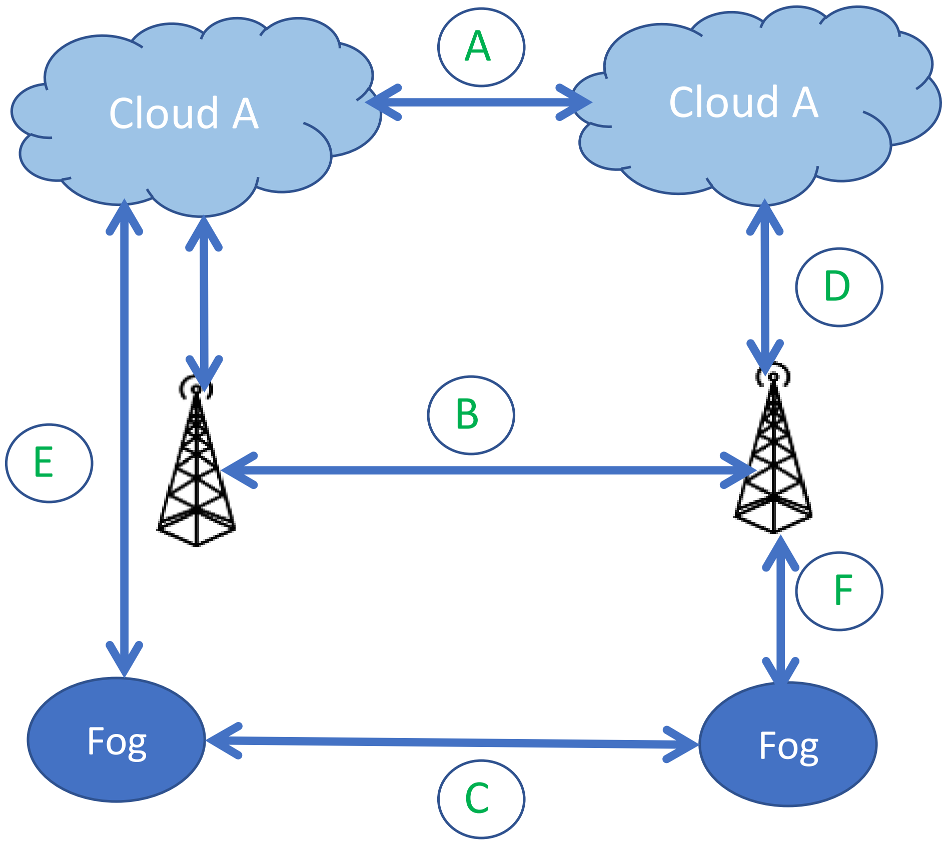
- Horizontal Federation
- Vertical Federation
    - Up-Link
        - 2-Tier Vertical Federation
            - ID in the upper tier
            - ID in the lower tier
        - 3-Tier Vertical Federation
            - ID in the upper tier
            - ID in the middle tier
            - ID in the lower tier
    - Down-Link
- Hybrid Federation
    - 2-Tier Federation
        - ID in the upper tier
        - ID in the lower tier
    - 3-Tier Federation
        - ID in the upper tier
        - ID in the middle tier
        - ID in the lower tier



- **Federation**
  - **Horizontal**
    - C-C
    - E-E
    - F-F
  - **Vertical**
    - **One-to-Many**
      - **2-Tier**
        - **ID-Upper**
          - **C**-E-E
          - **C**-F-F
          - **E**-F-F
        - **ID-Lower**
          - C-**E**-E
          - C-**F**-F
          - E-**F**-F
      - **3-Tier**
        - C-E-F
        - C-E-F
        - C-E-F
    - **Many-to-One**
      - C-E-C
      - C-F-C
      - E-F-E
  - **Hybrid**
    - **2-Tier**
      - **ID-Upper**
        - C-C-E
        - C-C-F
        - E-F-F
      - **ID-Lower**
        - C-C-E-E
        - C-C-F-F
        - E-E-F-F
    - **3-Tier**
      - C-E-F
      - C-E-F
      - C-E-F

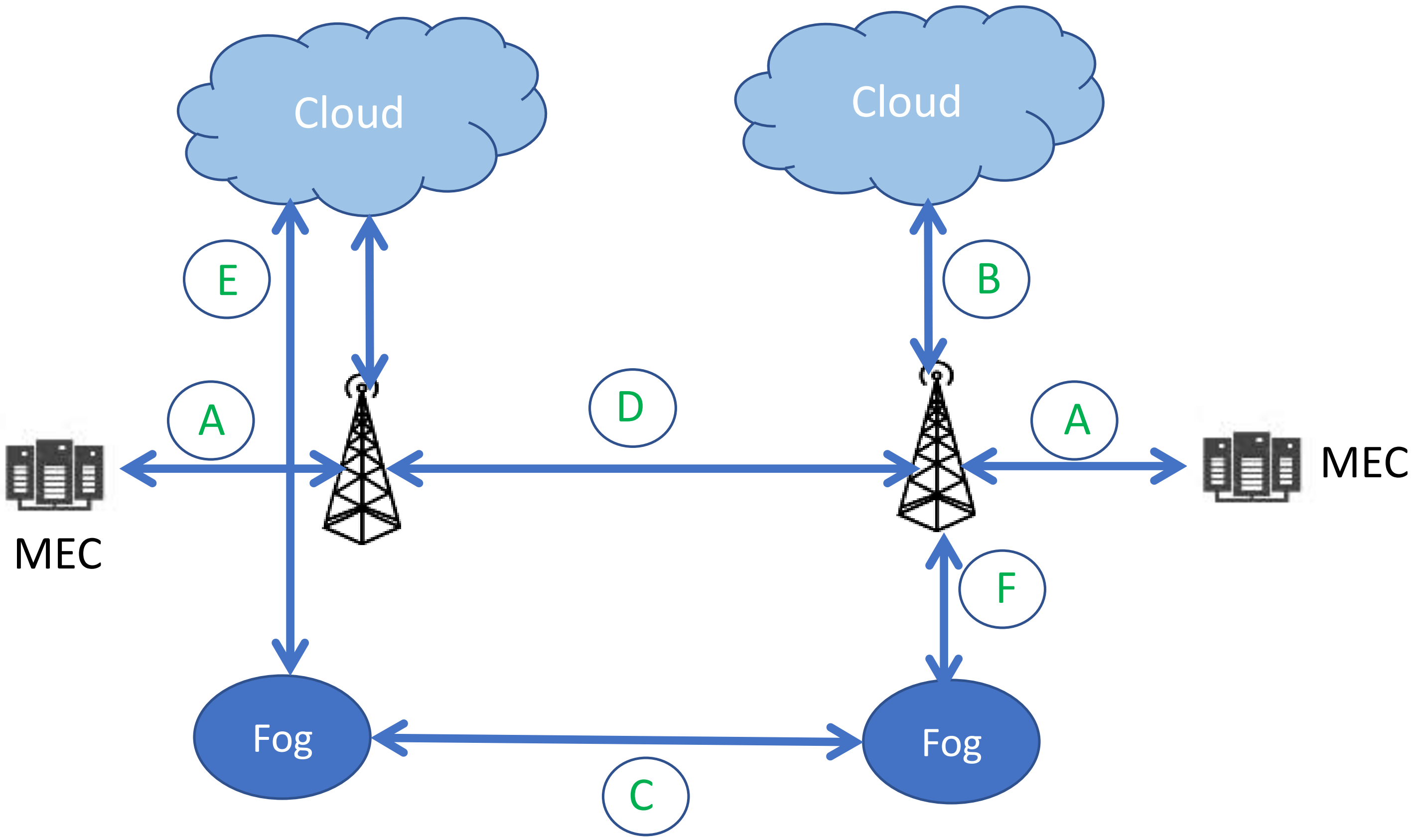
Protocols based Classification-I

- A: Cloud-Cloud
- B: Edge-Edge
- C: Fog-Fog
- D: Cloud-Edge
- E: Cloud-Fog
- F: Edge-Fog

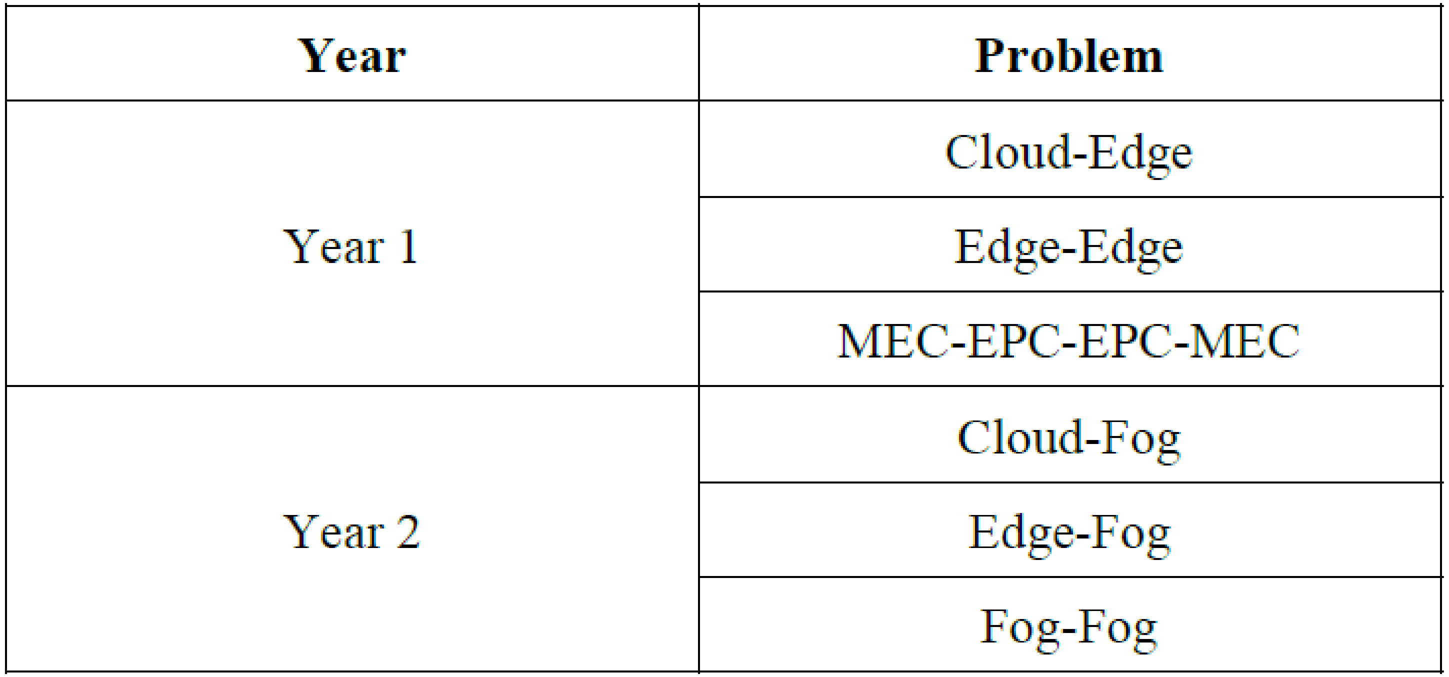


Federation Issues

- A: MEC-MEC
- B: Cloud-Edge
- C: Fog-Fog
- D: Edge-Edge
- E: Cloud-Fog
- F: Edge-Fog



Federation Problems



Year	Problem
Year 1	Cloud-Edge
	Edge-Edge
	MEC-EPC-EPC-MEC
Year 2	Cloud-Fog
	Edge-Fog
	Fog-Fog

Federation Survey -I

Name	How	What	All Federation Scenarios?	Transparent ?	Multiple protocols support?
Marcos et al [2]	Shibboleth	Multi-Tenancy	× [C—C]	✓	×
Antonio [3]	IDM/SP model	SSO	× [C—C]	× [Modified]	×
Antonio [4]	IDM/SP model	3-phase SSO	× [C—C]	× [Modified]	×
Zubair [5]	TPM	Federated ID	× [C—C]	× [Modified]	×
Liang [6]	FIM/HIBC	Mutual Auth	× [C—C]	× [Modified]	×
Maicon [7]	LDAP	FIM	× [C—C]	✓	×

Federation Survey-II

Name	How	What	All Federation Scenarios?	Transparent ?	Multiple Protocols Support?
Donald [8]	Centralized Infrastructure 3-p	Mutual Authentication	× [E-E]	× [New]	×
Ibrahim [9]	One master Key	Mutual Authentication	× [F-F]	× [New]	×
Shouhuai [10]	Whereabouts	Situational Authentication	× [Mobile Cloud]	× [New]	×
Bouzefrane [11]	NFC	Mutual Authentication	× [Mobile Cloud]	× [Modified]	×

Federation Survey-III

Name	How	What	All Federation Scenarios?	Transparent ?	Multiple Protocols Support?
SEGR [12]	certificateless aggregate signature	group roaming Authentication	× [F-E]	× [New]	×
MASFOG [13]	Blockchain	Mutual Authentication	× [F-E]	× [New]	×
Amor [14]	Pseudonym Based Cryptography	Mutual Authentication	× [F-E]	× [New]	×
Shidhani [15]	Modified EAP-AKA	Re-Authentication	× [F-E]	× [Modified]	×
Chen [16]	Vertical Handoff	QoS	× [F-E]	× [New]	×

Federation Survey-IV

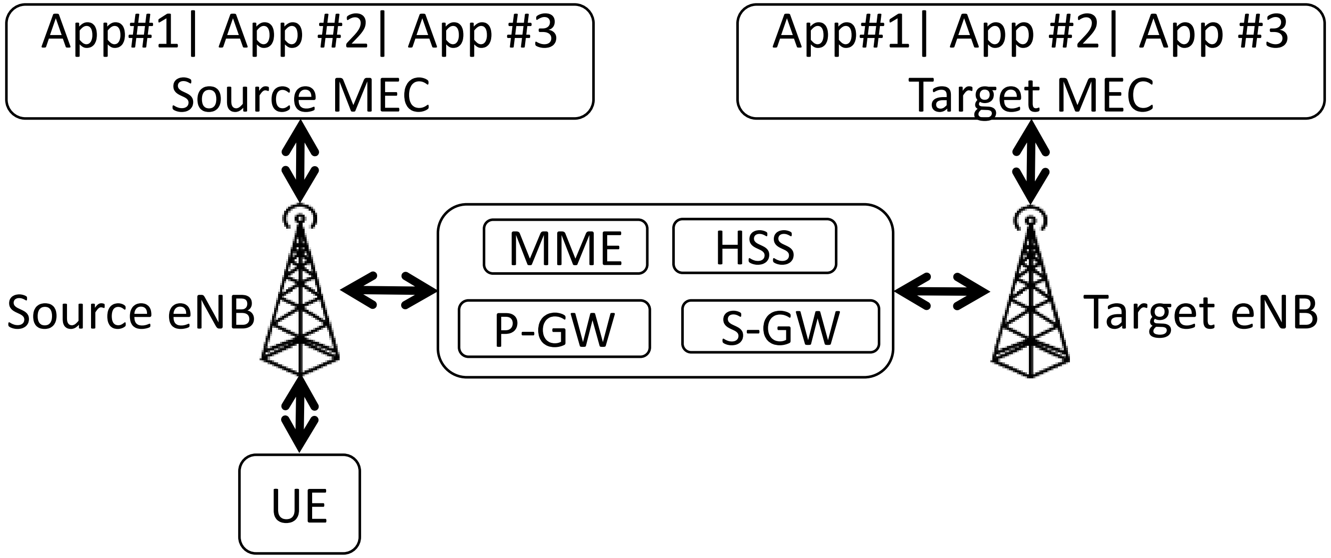
Name	How	What	All Federation Scenarios?	Transparent ?	Multiple Protocols Support
Hyeran [17]	Modified EAP-AKA	Mutual Authentication	× [F-E]	× [Modified]	×
Minghui [18]	Service Agent	Authentication /Billing	× [F-E]	× [New]	×
Yixin [19]	Secret Splitting	Mutual Authentication and Key Exchange	× [F-E]	× [New]	×
Minghui [20]	Mobile IP Handoff	Mutual Authentication	× [F-E]	× [Modified]	×
Sarang [21]	SDN	Security	×[F-C]	× [New]	×
Our Approach	Federation Proxy	Mutual Authentication	✓	✓	✓

service agent

802.11 roaming

Problem-I: Transparent 3rd-Party Authentication for Low-latency 5G Mobile Edge Computing with Mobility Support

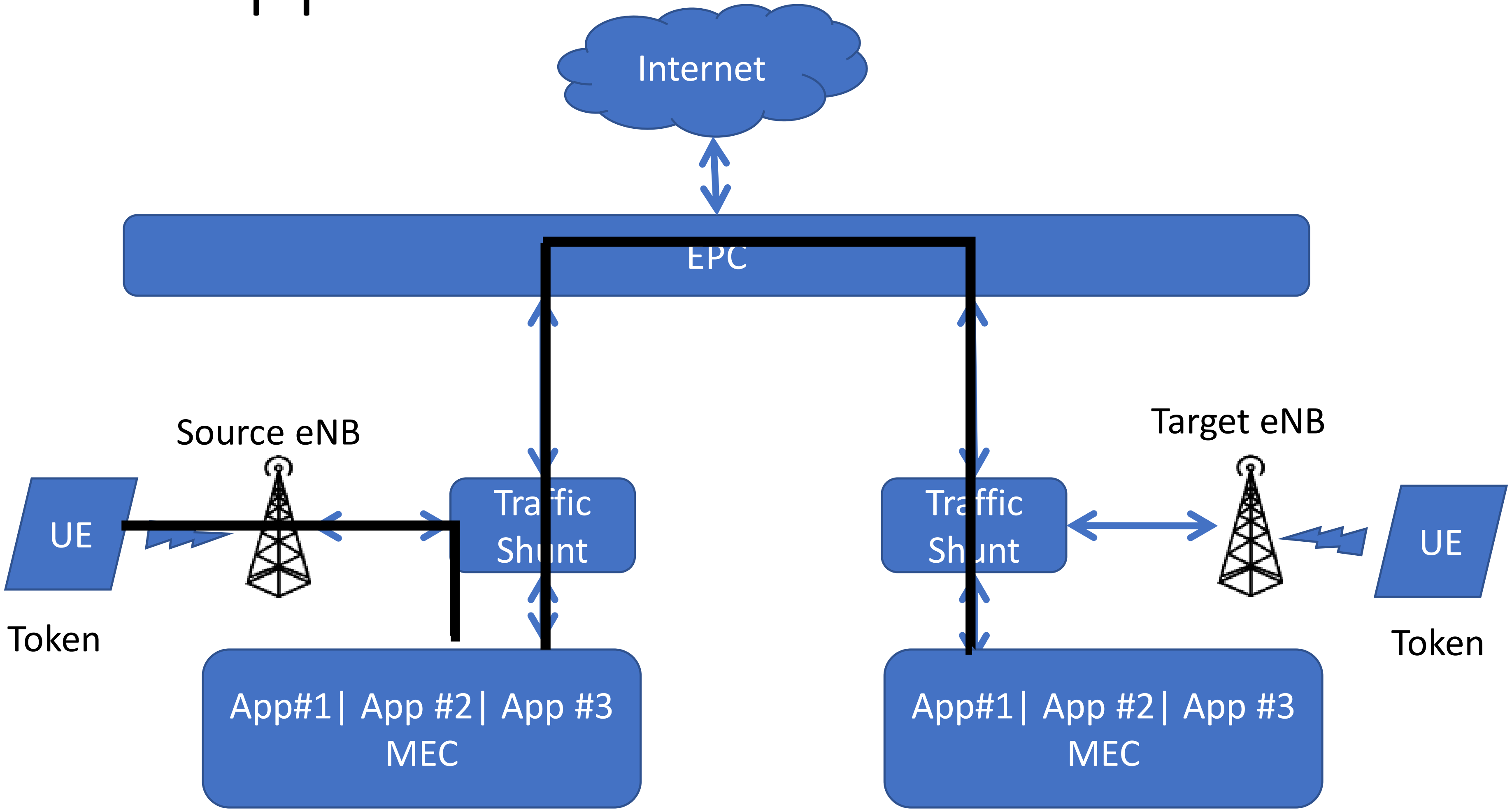
Problem Scenario



Problem Formulation

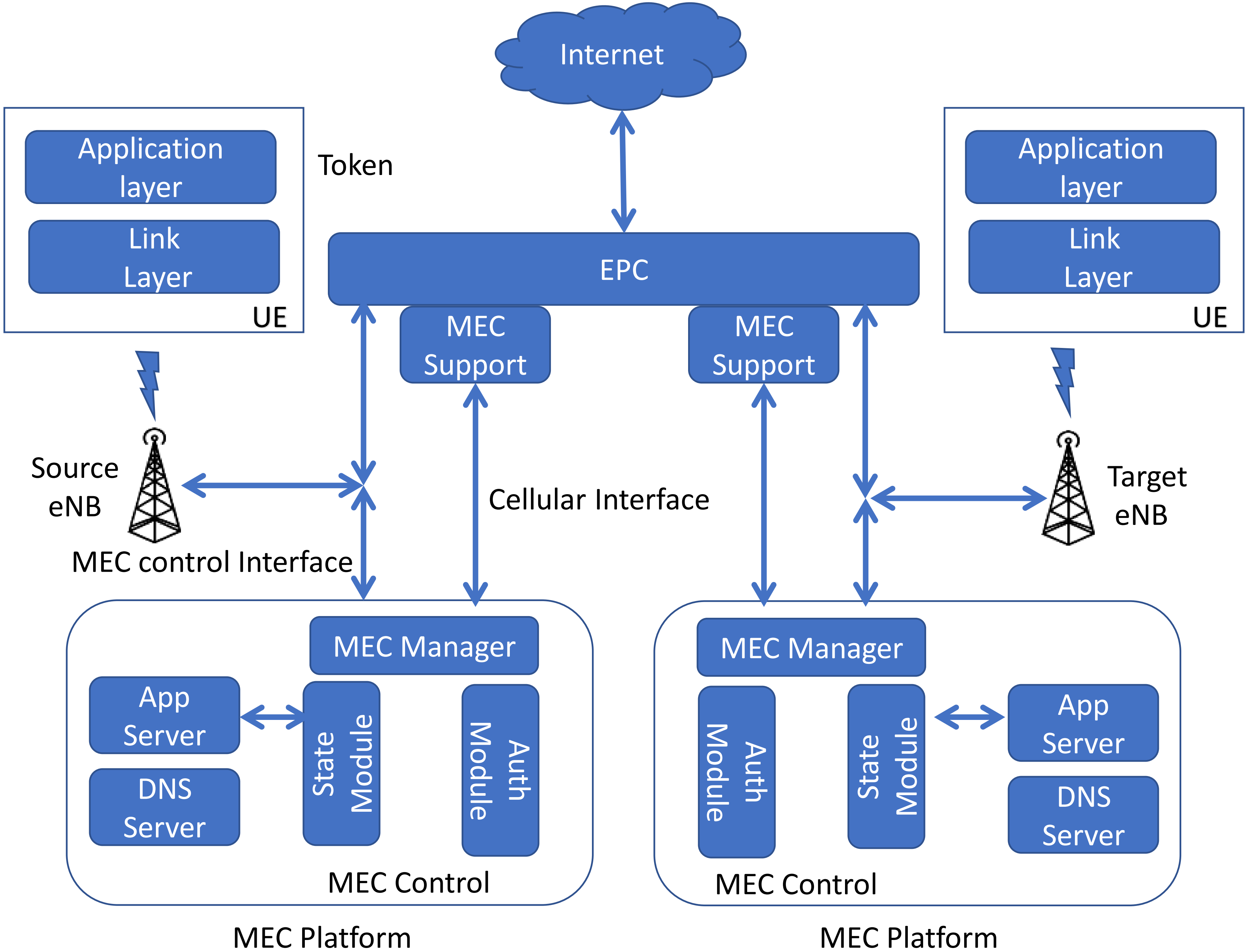
- **Given:**
  - Two MECs connected via existing 3GPP network.
  - UE is authenticated with source MEC initially.
  - UE Accesses App server in source MEC and moves towards target MEC while using same application.
  - Link layer handover triggers MEC handover.
  - Each MEC knows about the public keys of other MECs.
- **Objective:**
  - UE must access same application seamlessly from target MEC
- **Issues:**
  - Solve the issues while achieving low latency:
    - How to inform target MEC about source MEC.
    - How to authenticate the UE with target MEC.
    - How to transfer state information from MEC-1 App server to MEC-2 App server.

Solution Approach



A: State Information

Architecture

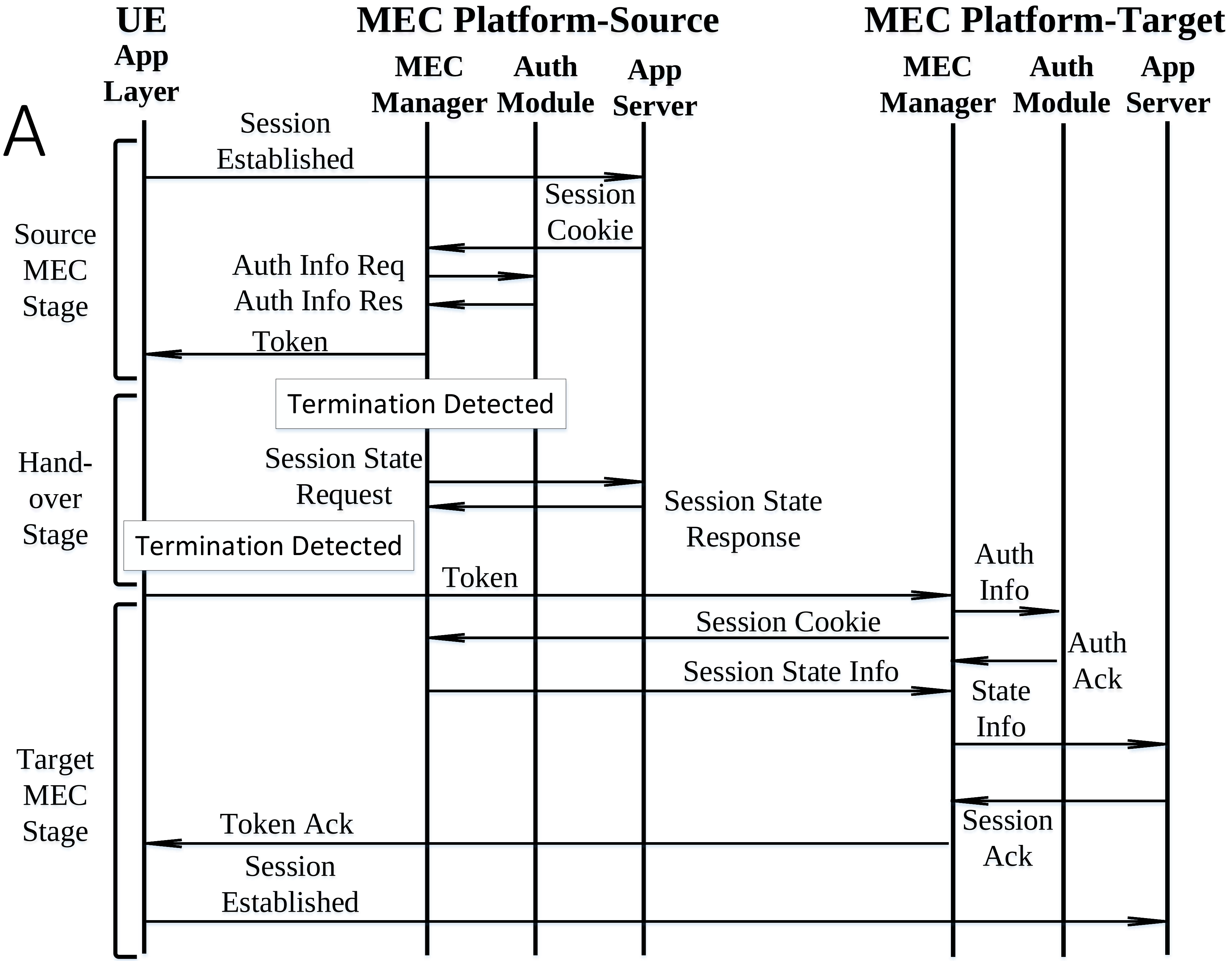

Internet
Application layer
Link Layer
UE
Token
EPC
MEC Support
MEC Support
Application layer
Link Layer
UE
Source eNB
MEC control Interface
Cellular Interface
Target eNB
MEC Manager
App Server
DNS Server
State Module
Auth Module
MEC Control
MEC Platform
MEC Manager
Auth Module
State Module
App Server
DNS Server
MEC Control
MEC Platform

Solution Approaches

- TC3A (Token-based Cookie transfer & 3rd-party Authentication)
  - Target MEC does not need to contact source MEC for the authentication but, needs to contact for session state
- TS3A (Token-based State transfer & 3rd-party Authentication)
  - Target MEC does not need to contact with the source MEC at all

Parameters	TC3A	TS3A
3-p Authentication	✓	✓
Cookie Transfer	✓	X
Session State Transfer	X	✓
Number of Tokens	1	N
Inter-MEC Connectivity	X	✓
Server Modification	Less	More

TC3A



UE

App Layer

MEC Platform-Source

MEC Manager

Auth Module

App Server

MEC Platform-Target

MEC Manager

Auth Module

App Server

Source MEC Stage

Session Established

Session Cookie

Auth Info Req

Auth Info Res

Token

Termination Detected

Hand-over Stage

Session State Request

Session State Response

Termination Detected

Token

Target MEC Stage

Auth Info

Session Cookie

Auth Ack

Session State Info

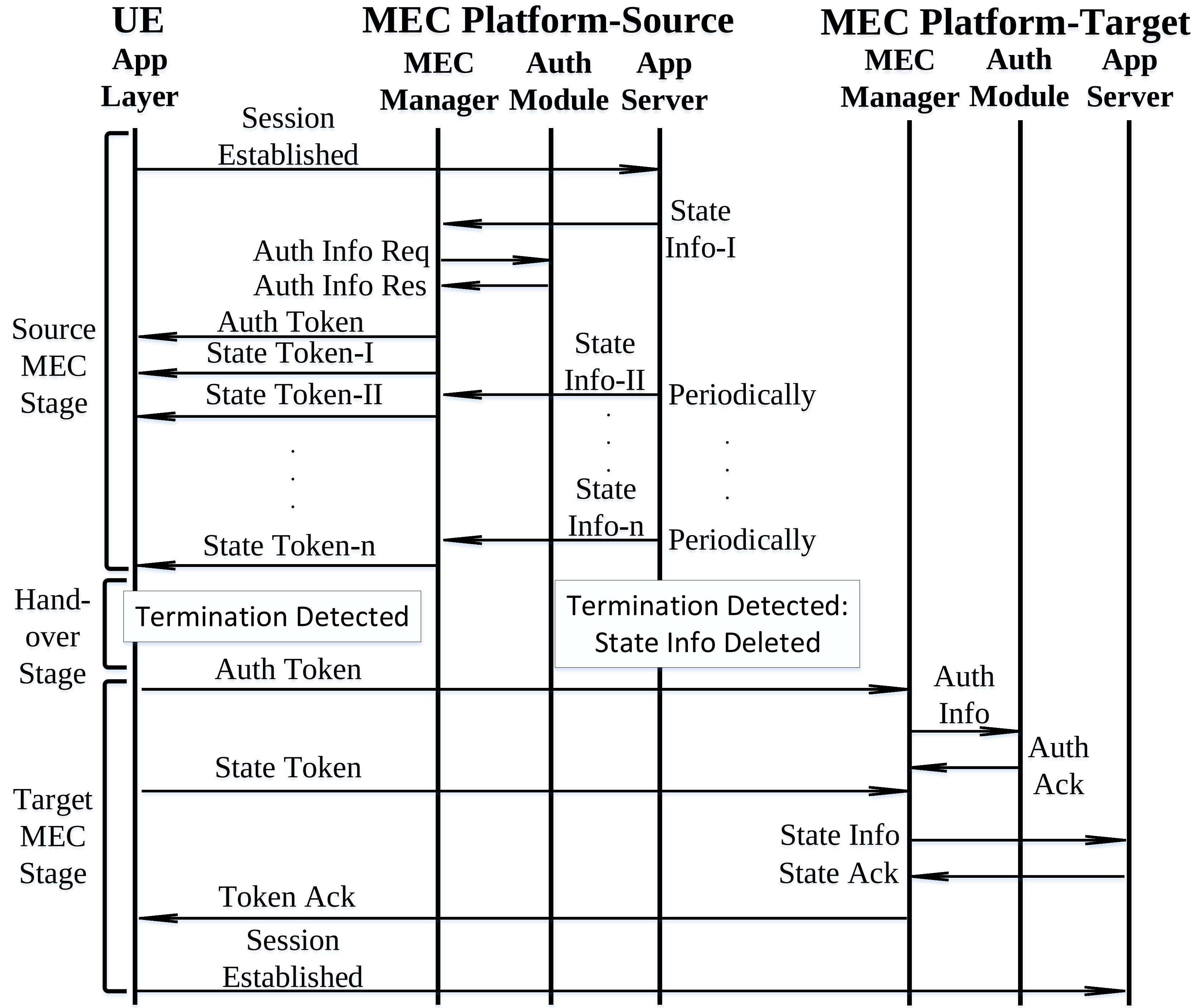
State Info

Session Ack

Token Ack

Session Established

TS3A



UE

App Layer

MEC Platform-Source

MEC Manager

Auth Module

App Server

MEC Platform-Target

MEC Manager

Auth Module

App Server

Source MEC Stage

Session Established

State Info-I

Auth Info Req

Auth Info Res

Auth Token

State Token-I

State Info-II

Periodically

State Token-II

. . .

. . .

. . .

State Info-n

Periodically

State Token-n

Hand-over Stage

Termination Detected

Termination Detected: State Info Deleted

Target MEC Stage

Auth Token

Auth Info

Auth Ack

State Token

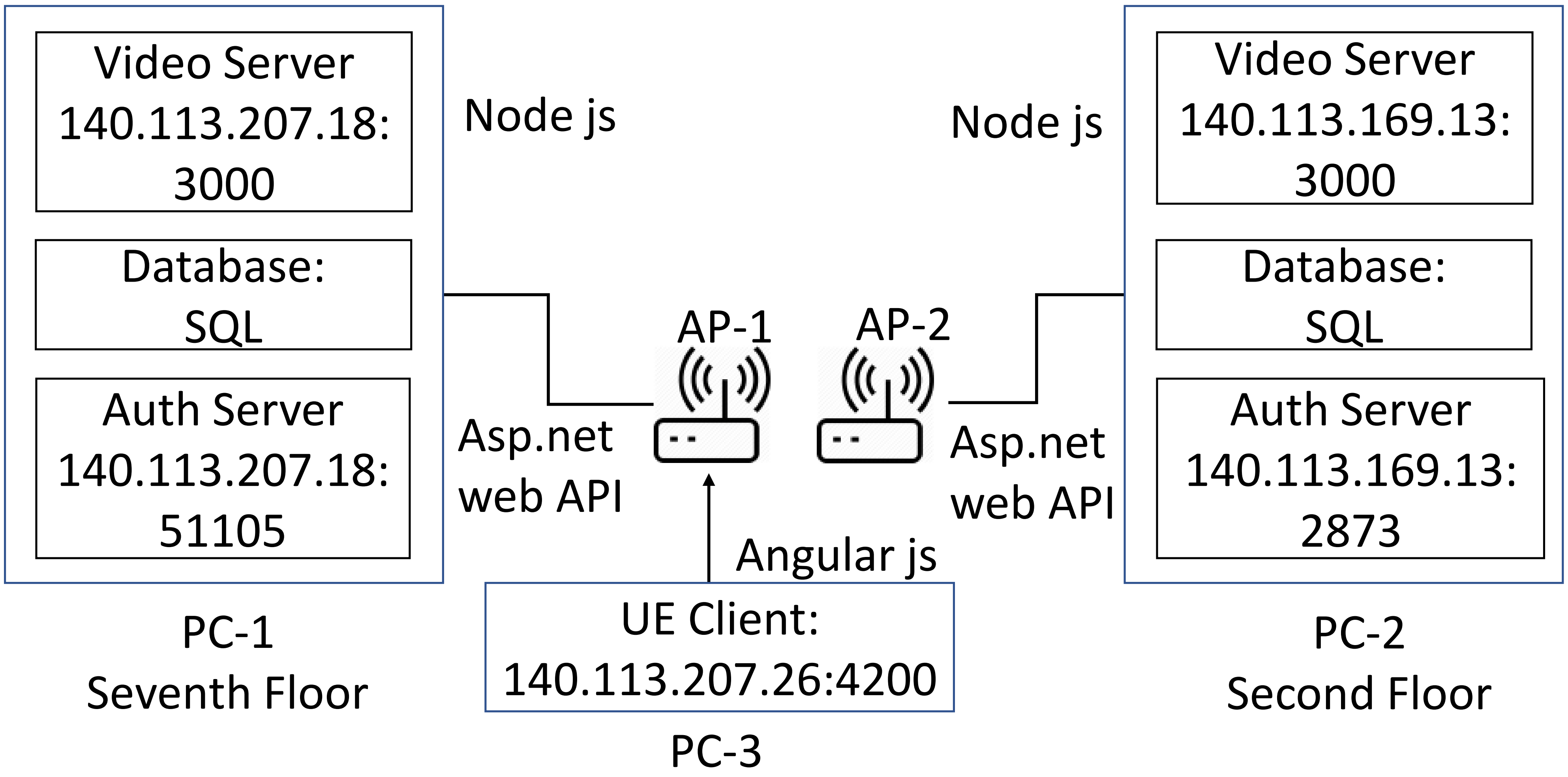
State Info

State Ack

Token Ack

Session Established

Experiment



Video Server
140.113.207.18:
3000

Database:
SQL

Auth Server
140.113.207.18:
51105

PC-1
Seventh Floor

Node js

Asp.net
web API

AP-1

AP-2

Angular js

UE Client:
140.113.207.26:4200

PC-3

Node js

Asp.net
web API

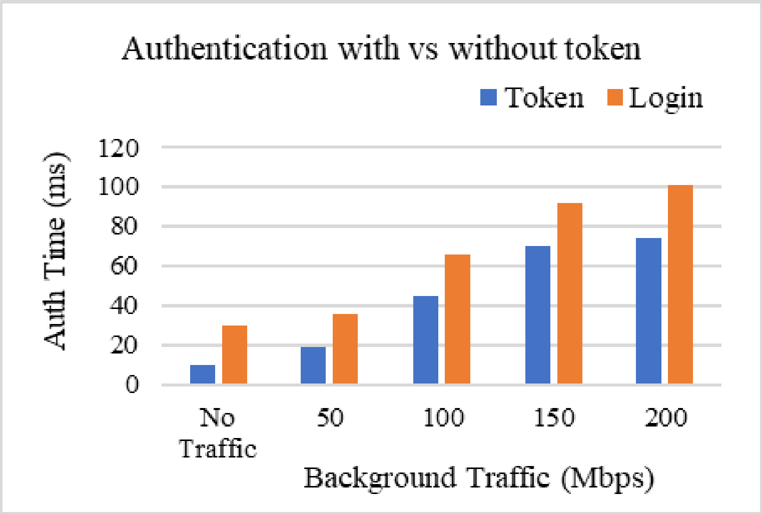
Video Server
140.113.169.13:
3000

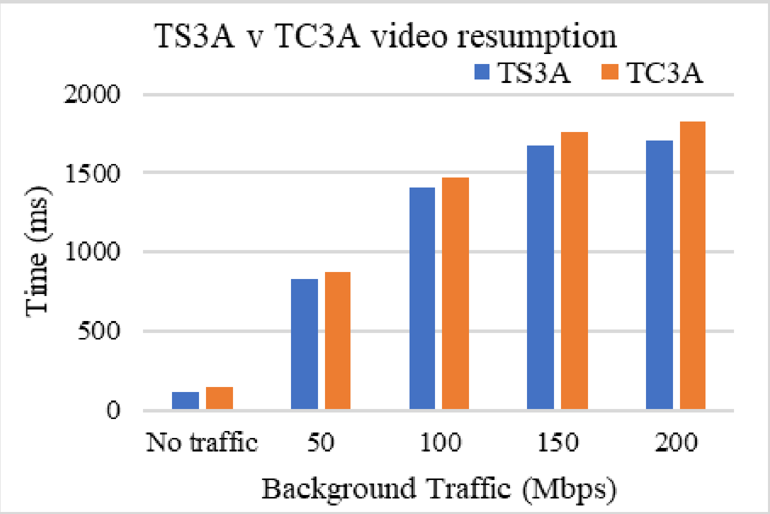
Database:
SQL

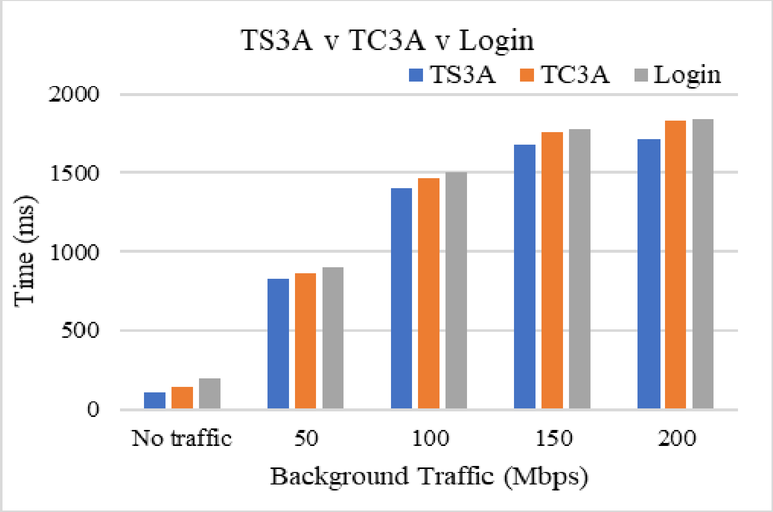
Auth Server
140.113.169.13:
2873

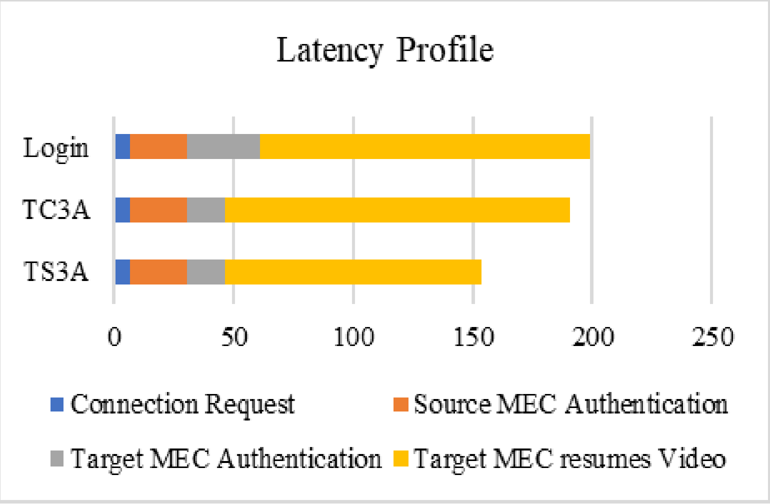
PC-2
Second Floor

Results


Authentication with vs without token
Token
Login
Auth Time (ms)
120
100
80
60
40
20
0
No Traffic
50
100
150
200
Background Traffic (Mbps)


TS3A v TC3A video resumption
TS3A
TC3A
Time (ms)
2000
1500
1000
500
0
No traffic
50
100
150
200
Background Traffic (Mbps)


TS3A v TC3A v Login
TS3A
TC3A
Login
Time (ms)
2000
1500
1000
500
0
No traffic
50
100
150
200
Background Traffic (Mbps)


Latency Profile
Login
TC3A
TS3A
0
50
100
150
200
250
Connection Request
Source MEC Authentication
Target MEC Authentication
Target MEC resumes Video

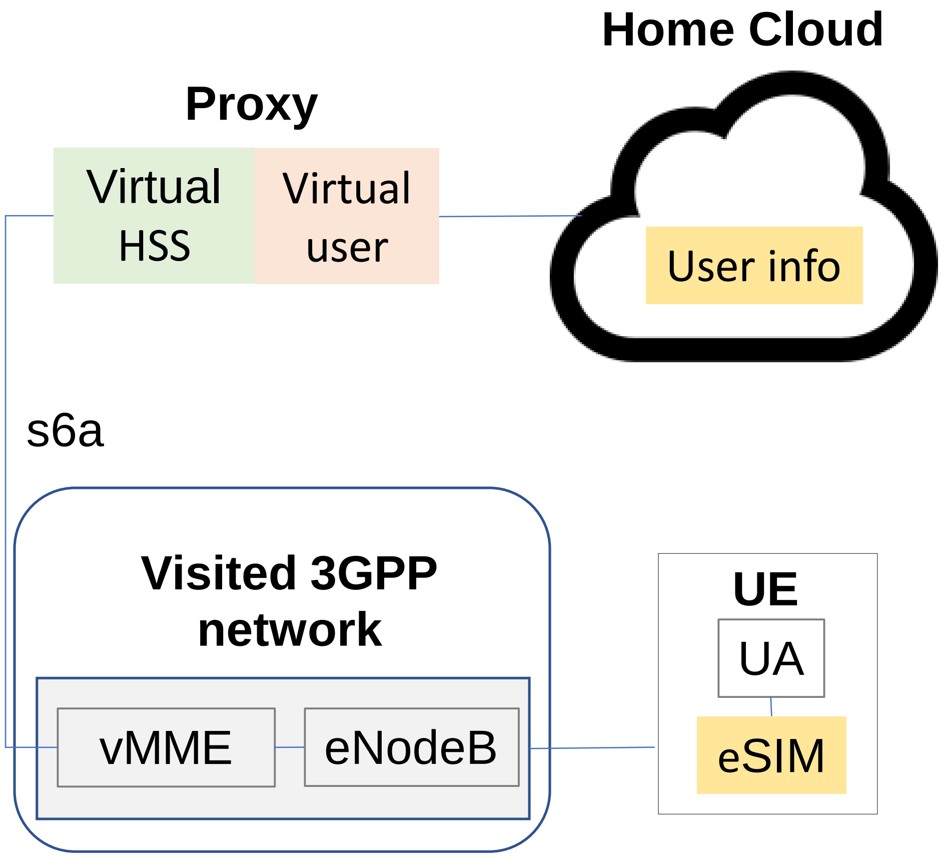
Problem-II: 3rd-Party Authentication in Federated Cloud and 3GPP systems

Problem

- How third party authenticate user?
  - UE has no account on third party
  - UE does not want to register an account on third party
- How 3GPP network communicate with cloud?
  - Different authentication protocols
- Cloud-to-edge scenario
- Edge-to-cloud scenario
- Solution: Proxy

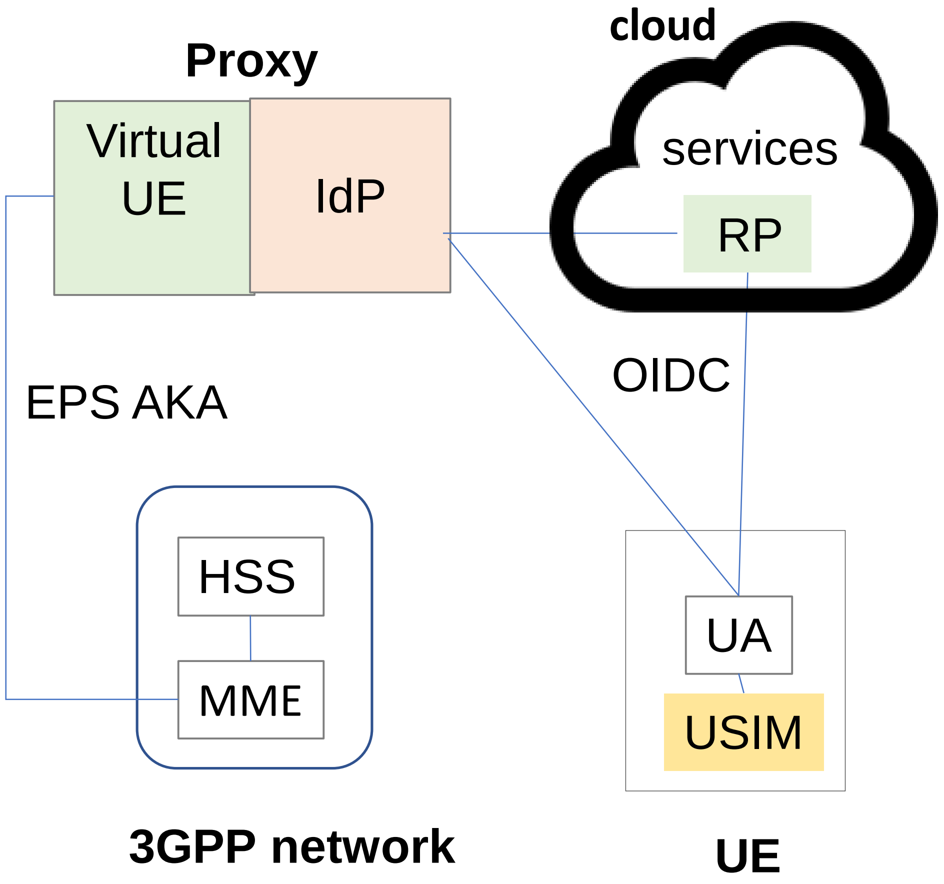
Proxy: cloud-to-edge scenario

Virtual HSS	Virtual user
- Act as the home HSS - Communicate with 3GPP network	- Established a connection to home cloud on the Internet - Perform mutual authentication



Proxy: edge-to-cloud scenario

IdP	Virtual UE
- Act as the identity provider in OIDC protocol. - Communicate with cloud	- emulated typical UE - Communicate with 3GPP network

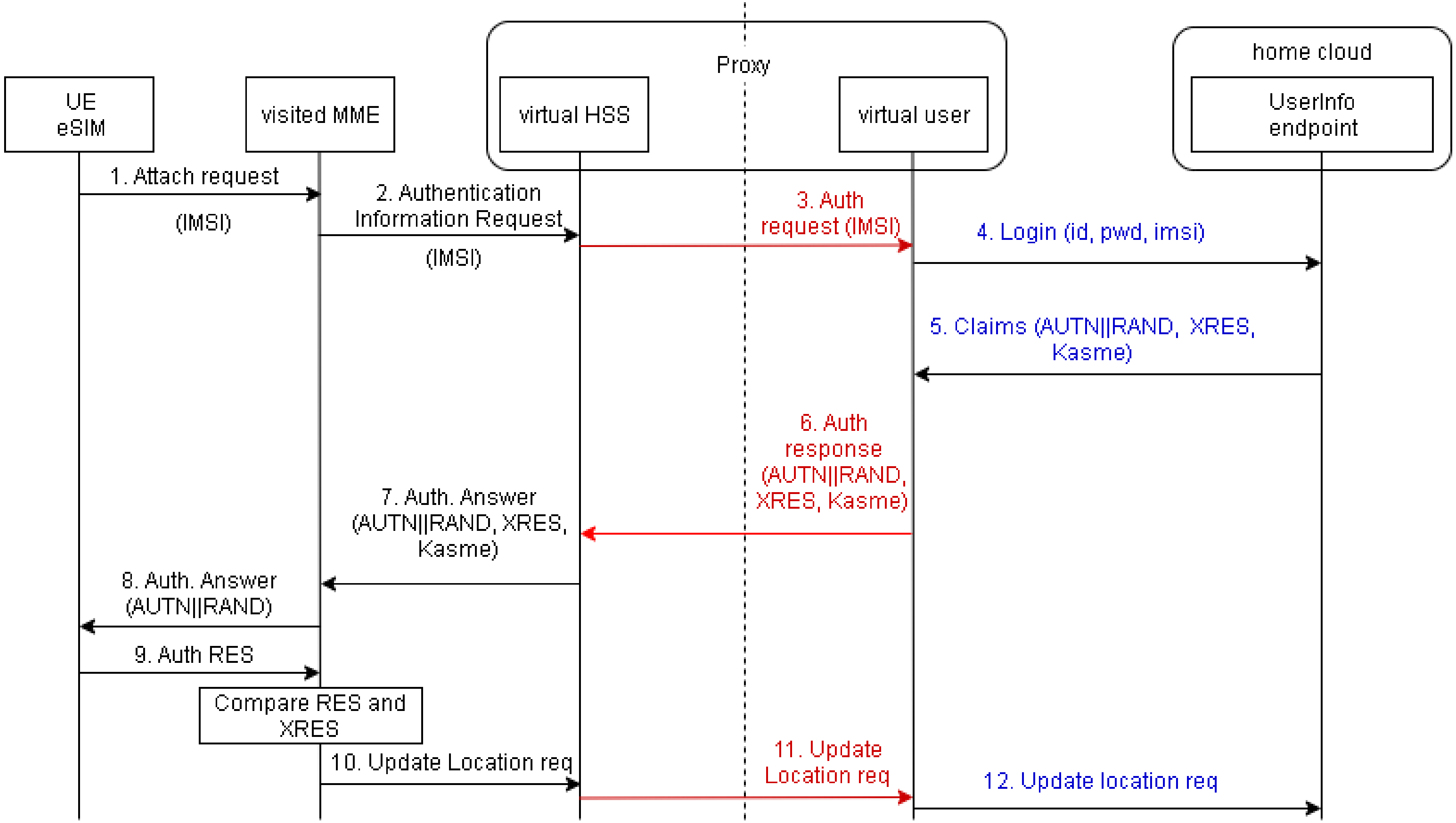


Cloud-to-Edge Solution

Stage 1:
auth. Info
req.

Stage 2:
auth. Info
res.

Stage 3:
auth.
confirmation



Proxy

home cloud

UE
eSIM

visited MME

virtual HSS

virtual user

UserInfo
endpoint

1. Attach request

(IMSI)

2. Authentication
Information Request

(IMSI)

3. Auth
request (IMSI)

4. Login (id, pwd, imsi)

5. Claims (AUTN||RAND, XRES,
Kasme)

6. Auth
response
(AUTN||RAND,
XRES, Kasme)

7. Auth. Answer
(AUTN||RAND, XRES,
Kasme)

8. Auth. Answer
(AUTN||RAND)

9. Auth RES

Compare RES and
XRES

10. Update Location req

11. Update
Location req

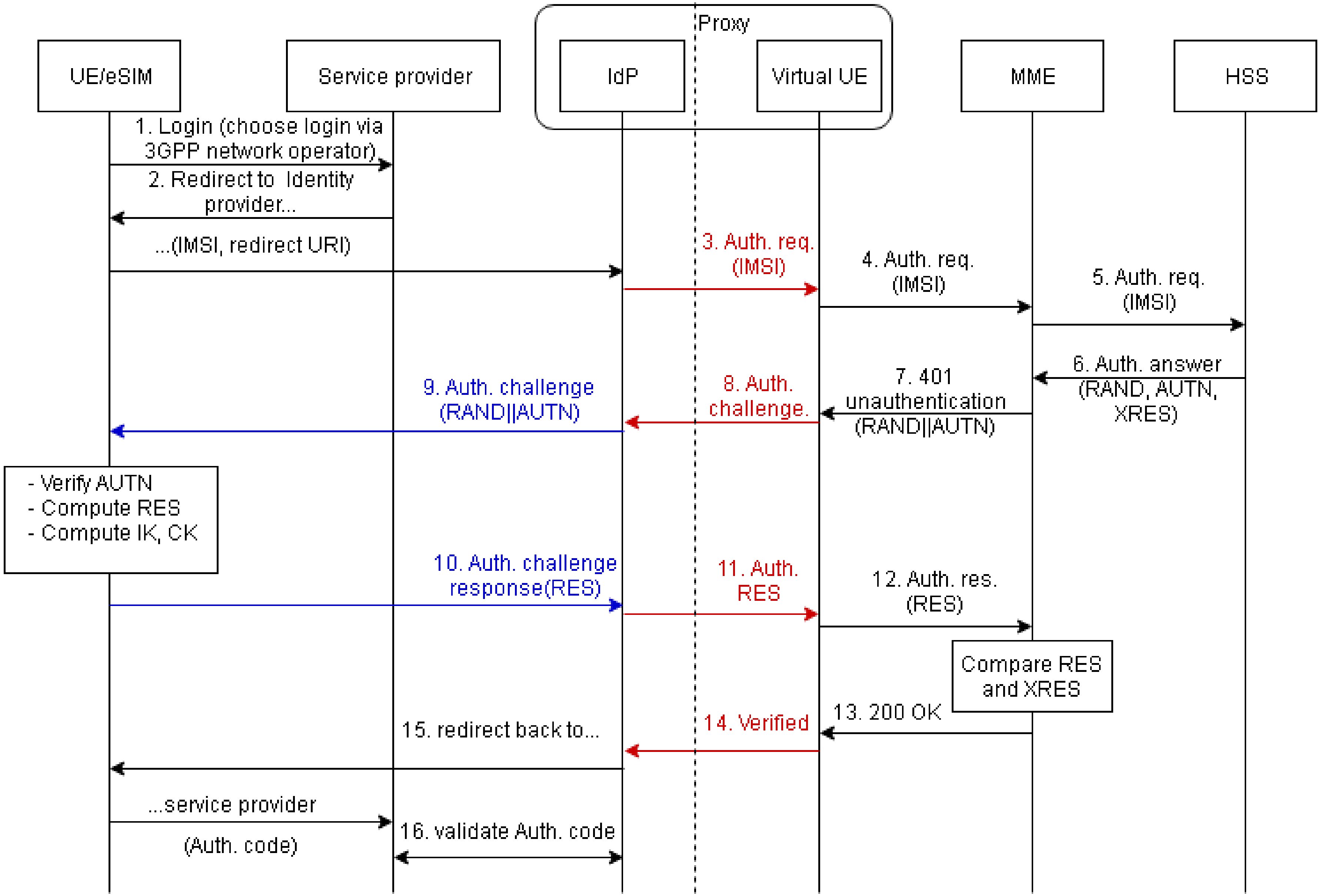
12. Update location req

Edge-to-Cloud Solution

Stage 1:
auth. Info
req.

Stage 2:
auth. Info
res.

Stage 3:
auth.
confirmation



Proxy

UE/eSIM

Service provider

IdP

Virtual UE

MME

HSS

1. Login (choose login via 3GPP network operator)

2. Redirect to Identity provider...

...(IMSI, redirect URI)

3. Auth. req. (IMSI)

4. Auth. req. (IMSI)

5. Auth. req. (IMSI)

6. Auth. answer (RAND, AUTN, XRES)

7. 401 unauthentication (RAND||AUTN)

8. Auth. challenge.

9. Auth. challenge (RAND||AUTN)

- Verify AUTN
- Compute RES
- Compute IK, CK

10. Auth. challenge response(RES)

11. Auth. RES

12. Auth. res. (RES)

Compare RES and XRES

13. 200 OK

14. Verified

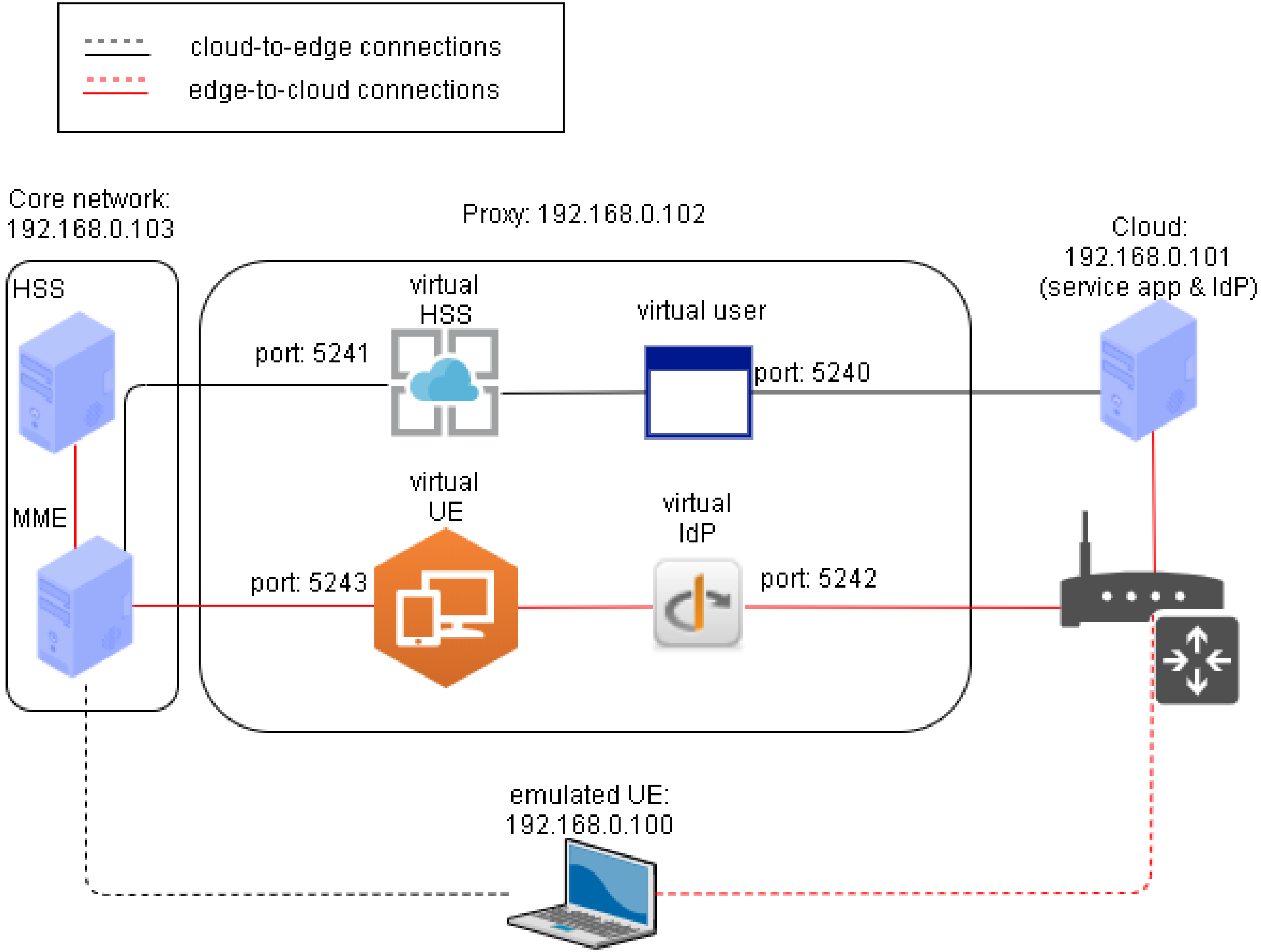
15. redirect back to...

...service provider

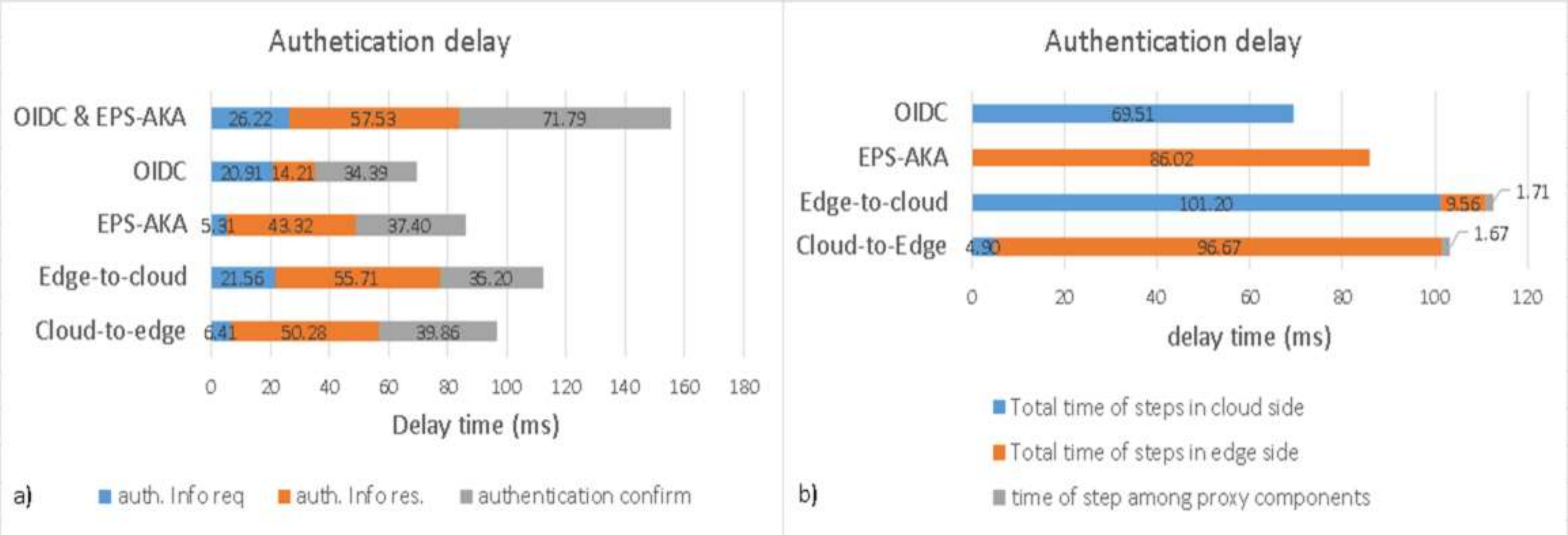
(Auth. code)

16. validate Auth. code

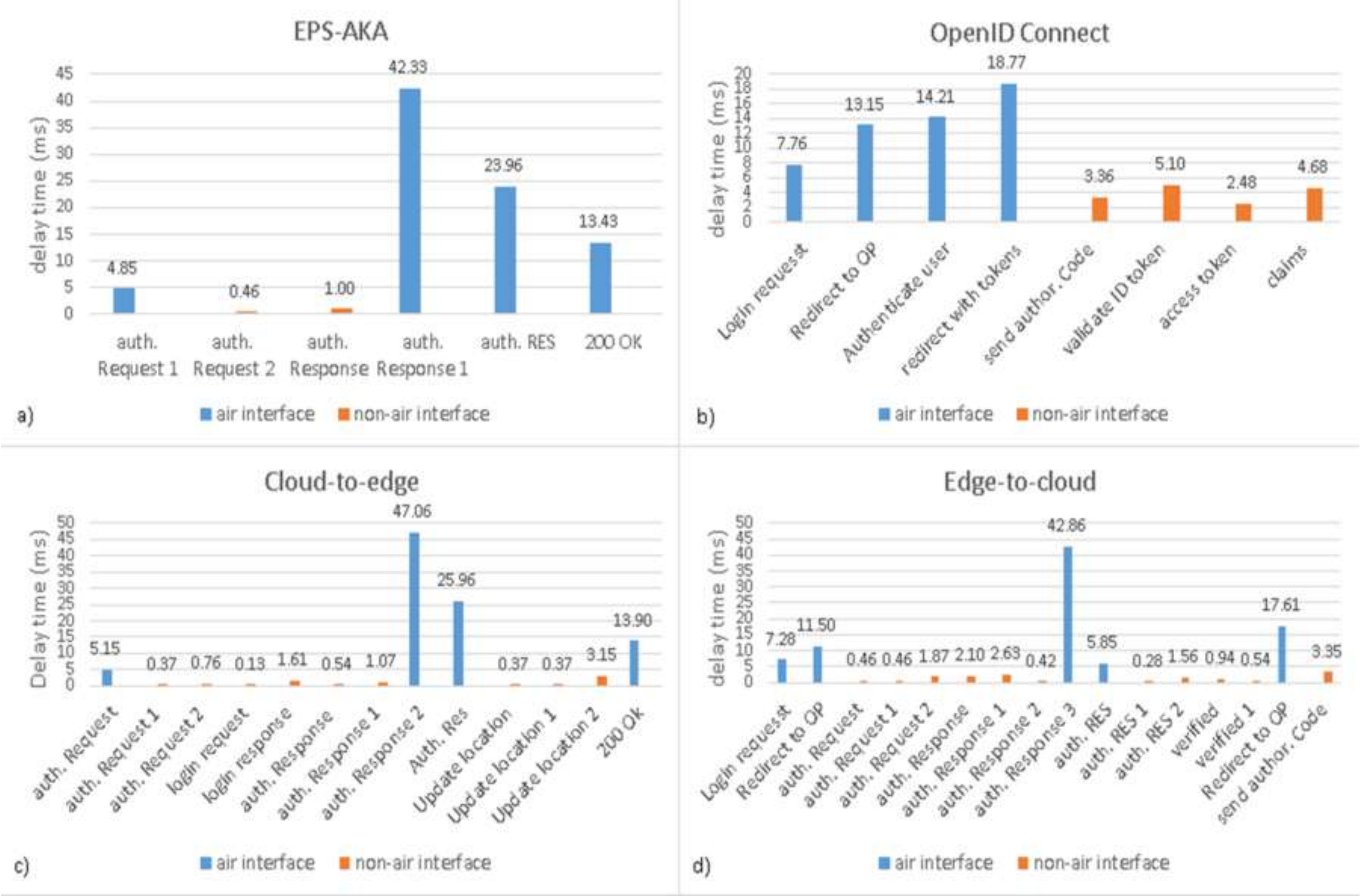
Testbed


cloud-to-edge connections
edge-to-cloud connections
Core network:
192.168.0.103
Proxy: 192.168.0.102
Cloud:
192.168.0.101
(service app & IdP)
HSS
MME
virtual
HSS
port: 5241
virtual user
port: 5240
virtual
UE
port: 5243
virtual
IdP
port: 5242
emulated UE:
192.168.0.100

Delay time


Authetication delay
OIDC & EPS-AKA
26.22
57.53
71.79
OIDC
20.91
14.21
34.39
EPS-AKA
5.31
43.32
37.40
Edge-to-cloud
21.56
55.71
35.20
Cloud-to-edge
6.41
50.28
39.86
0
20
40
60
80
100
120
140
160
180
Delay time (ms)
a)
🟦 auth. Info req
🟧 auth. Info res.
⬜ authentication confirm
Authentication delay
OIDC
69.51
EPS-AKA
86.02
Edge-to-cloud
101.20
9.56
1.71
Cloud-to-Edge
4.90
96.67
1.67
0
20
40
60
80
100
120
delay time (ms)
🟦 Total time of steps in cloud side
🟧 Total time of steps in edge side
⬜ time of step among proxy components
b)

Delay time


EPS-AKA
delay time (ms)
45
40
35
30
25
20
15
10
5
0
4.85
0.46
1.00
42.33
23.96
13.43
auth. Request 1
auth. Request 2
auth. Response
auth. Response 1
auth. RES
200 OK
a)
air interface
non-air interface
OpenID Connect
delay time (ms)
20
18
16
14
12
10
8
6
4
2
0
7.76
13.15
14.21
18.77
3.36
5.10
2.48
4.68
Login requesst
Redirect to OP
Authenticate user
redirect with tokens
send author. Code
validate ID token
access token
claims
b)
air interface
non-air interface
Cloud-to-edge
Delay time (ms)
50
45
40
35
30
25
20
15
10
5
0
5.15
0.37
0.76
0.13
1.61
0.54
1.07
47.06
25.96
0.37
0.37
3.15
13.90
auth. Request
auth. Request 1
auth. Request 2
login request
login response
auth. Response
auth. Response 1
auth. Response 2
Auth. Res
Update location
Update location 1
Update location 2
200 Ok
c)
air interface
non-air interface
Edge-to-cloud
delay time (ms)
50
45
40
35
30
25
20
15
10
5
0
7.28
11.50
0.46
0.46
1.87
2.10
2.63
0.42
42.86
5.85
0.28
1.56
0.94
0.54
17.61
3.35
Login requesst
Redirect to OP
auth. Request
auth. Request 1
auth. Request 2
auth. Response
auth. Response 1
auth. Response 2
auth. Response 3
auth. RES
auth. RES 1
auth. RES 2
verified
verified 1
Redirect to OP
send author. Code
d)
air interface
non-air interface

What’s Next?

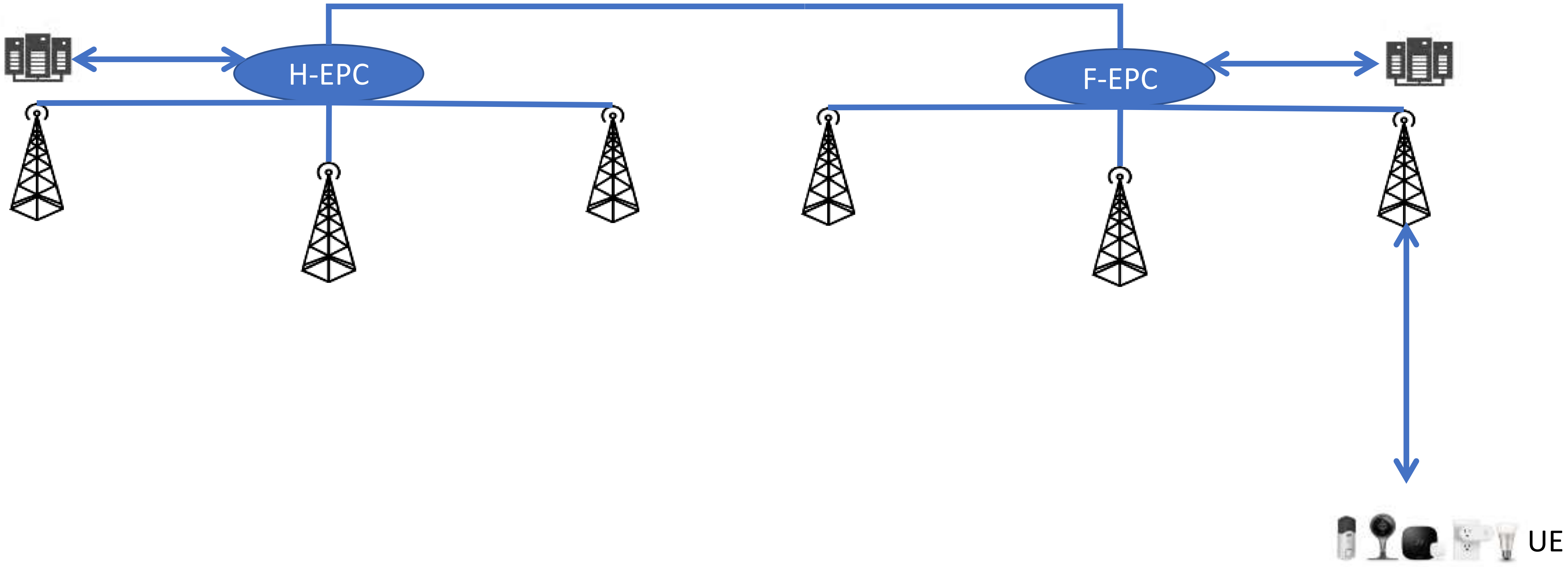
- Problem-III: Federated Edge-Edge Problem
- Problem-IV: Federated Cloud-Fog Problem

Problems Overview:

Problem Name	Solved?	Authentication	Application Handover	Protocols	Proxy	Proxy Roles
Cloud-Edge	✓	✓	X	OIDC,3GPP	✓	HSS, IdP, UE, Client
MEC-Edge	✓	✓	✓	Novel	X	X
Edge-Edge	x	✓	X	3GPP	X	--
Cloud-Fog	x	✓	✓	OIDC, Multiple Protocols	✓	--

Problem-III: Transparent 3rd-Party Authentication in Federated 3GPP systems

Problem Scenario



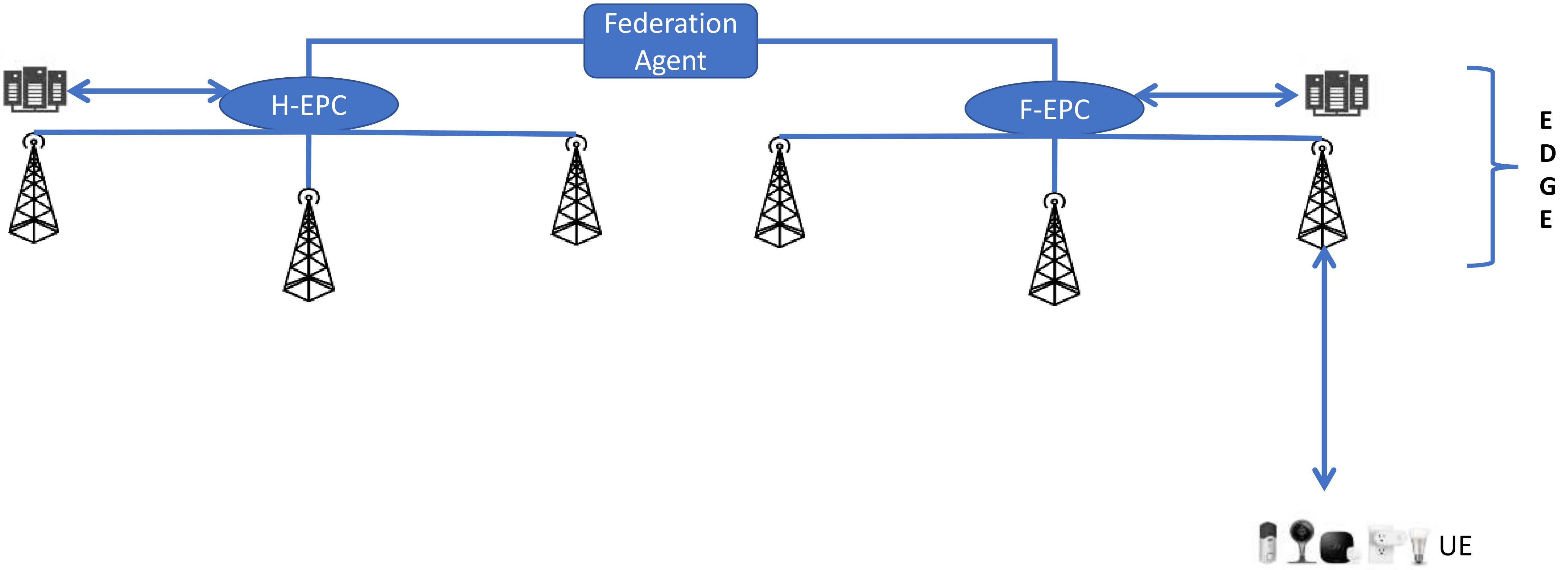
Problem Formulation

- **Given:**
  - Two 3GPP network connected to each other for roaming purposes.
  - UE is authenticated with home EPC initially.
  - UE Accesses computational services provided by the home 3GPP network and moves to the foreign 3GPP network and wants to access computational service.
- **Objective:**
  - UE must access computational services provided by foreign 3GPP network without having to make another account.
- **Issues:**
  - Solve the issues while achieving low latency:
    - How to authenticate UE with the computational services provided by foreign 3GPP network.
    - How to authenticate the UE with foreign 3GPP.

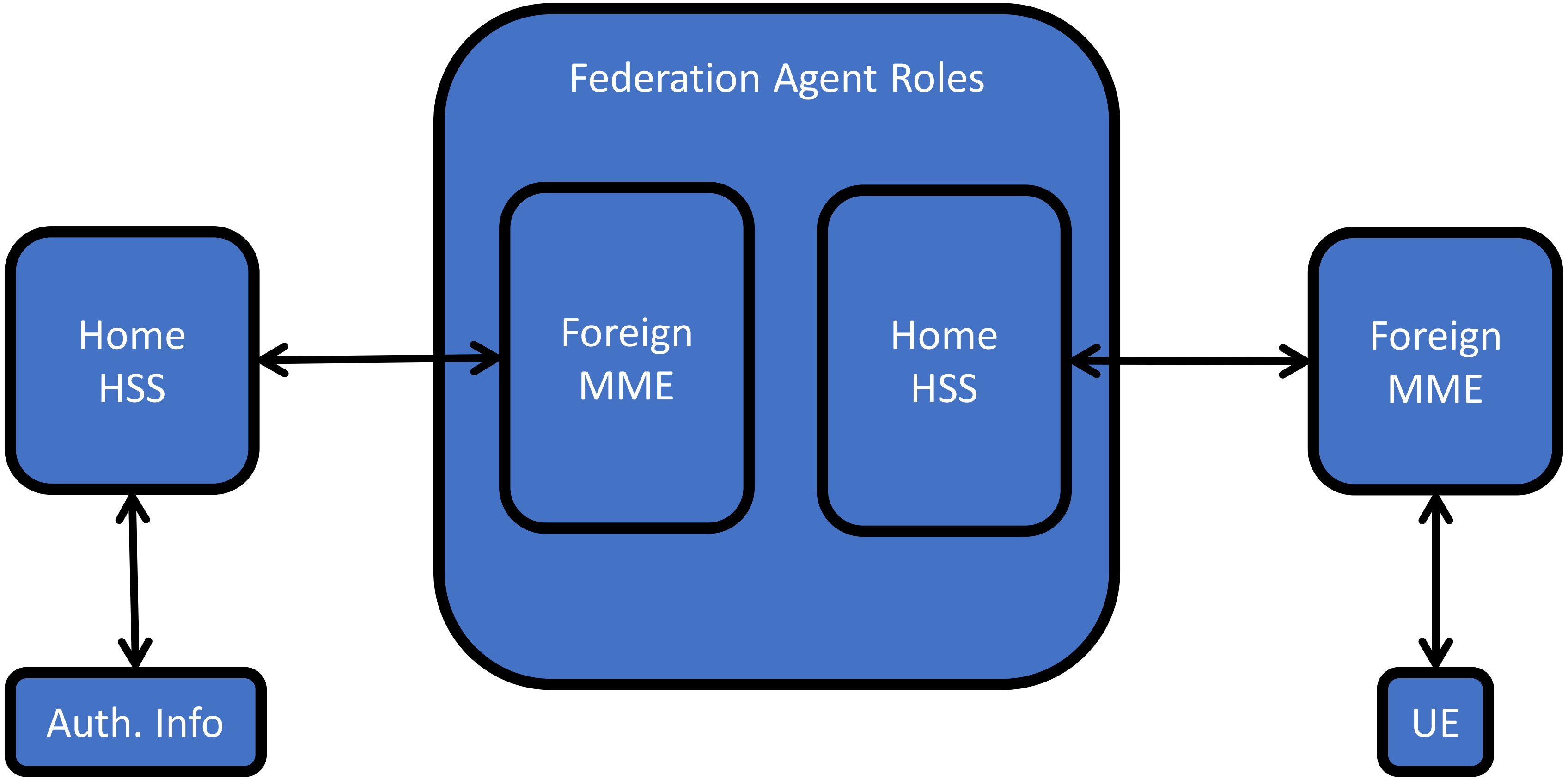
Survey

Name	Method	Problem	All Federation Scenarios?	Transparent?
Donald [8]	Centralized Infrastructure 3-p	Mutual Authentication	× [E-E]	× [New]
Yousaf [22]	Federated ID Systems	Seamless Authentication	X [E-WLAN]	X [Modified]
Vinod [23]	Multi factor Auth Proxy	Seamless Authentication	Multiple service providers	X
Joyce [24]	Open SDNCore	Infrastructure cloudification	X [E-E]	X

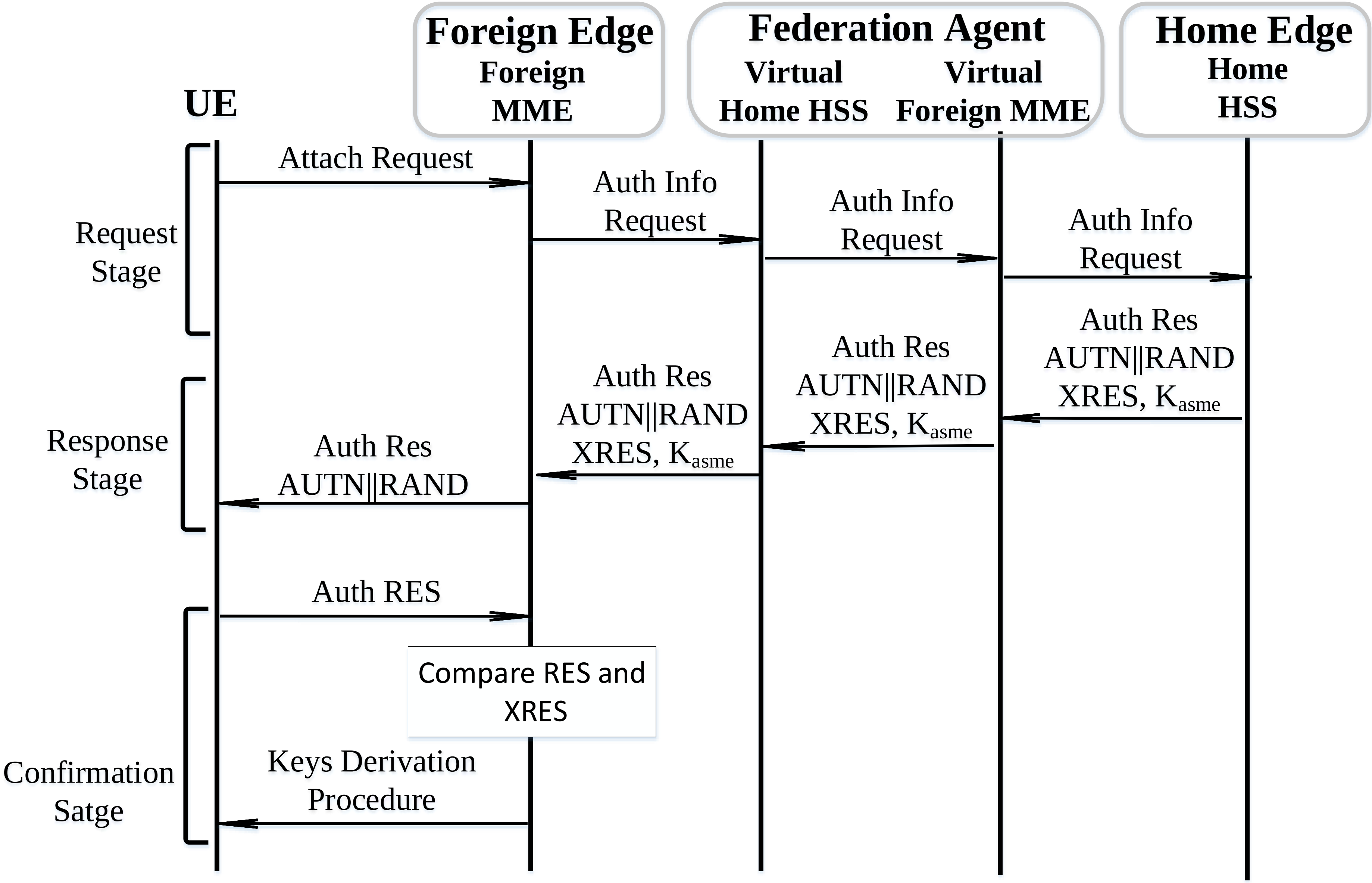
Proposed Solution-I



Proposed Solution-II



Proposed Solution-IV



Foreign Edge
Foreign MME

Federation Agent
Virtual Home HSS
Virtual Foreign MME

Home Edge
Home HSS

UE

Request Stage

Attach Request

Auth Info Request

Auth Info Request

Auth Info Request

Response Stage

Auth Res AUTN||RAND XRES, K_{asme}

Auth Res AUTN||RAND XRES, K_{asme}

Auth Res AUTN||RAND XRES, K_{asme}

Auth Res AUTN||RAND

Confirmation Satge

Auth RES

Compare RES and XRES

Keys Derivation Procedure

Pending Issues

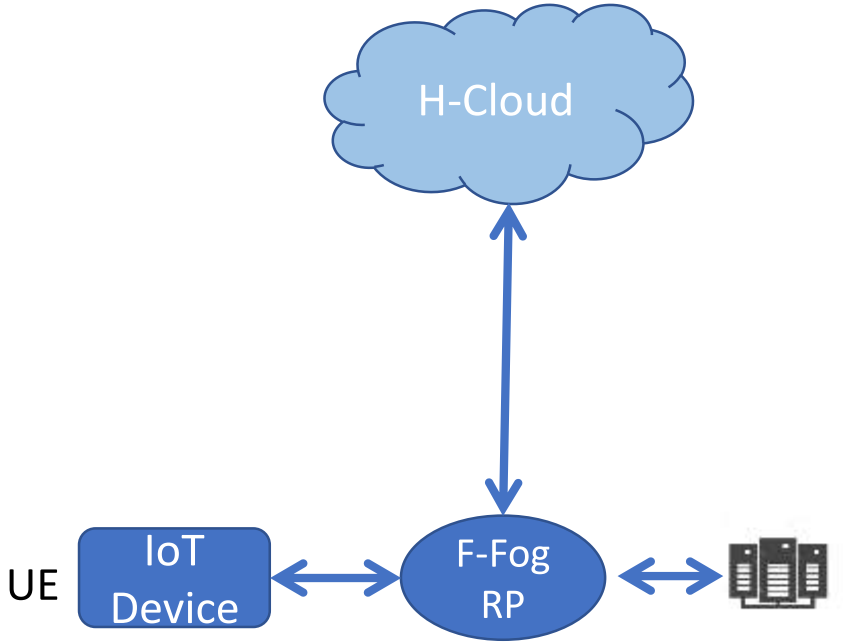
- Application handover through state transfer

The important things to read

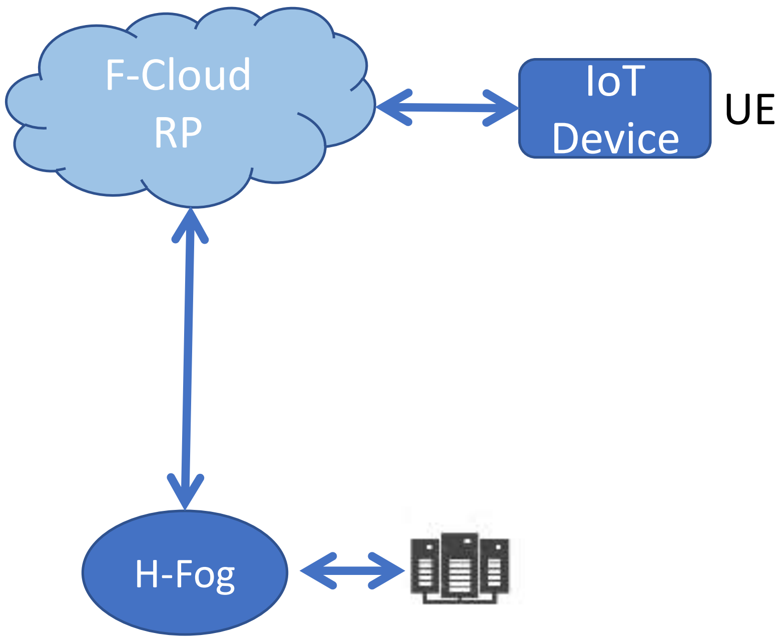
- Must understand the working of EPS-AKA
- Must understand the S6a interface in 3GPP LTE architecture
- Must understand the procedure of Roaming
- Must understand the state transfer

Problem-IV: Transparent 3rd-Party Authentication in Federated Cloud and Fog systems with Application Mobility Support

Problem Scenario



C-F Scenario



F-C Scenario

Problem Formulation [C-F]

- **Given:**
  - A Cloud connected with the fog device.
  - UE is authenticated with cloud initially.
  - UE Accesses computational services provided by the home cloud and moves to the foreign fog device and wants to access computational services.
- **Objective:**
  - UE must access computational services provided by foreign fog device without having to make another account.
  - UE must also be provided with the seamless application mobility.
- **Issues:**
  - Solve the issues while achieving low latency:
    - How to authenticate UE with the computational services provided by foreign fog network.
    - How to authenticate the UE with foreign fog.
    - How to communicate between fog and cloud.

UE should get service even in mobility

Problem Formulation[F-C]

- **Given:**
  - A cloud connected with the fog device.
  - UE is authenticated with home fog device.
  - UE Accesses computational services provided by the home fog device and moves to the foreign cloud and wants to access computational services.
- **Objective:**
  - UE must access computational services provided by foreign cloud without having to make another account.
  - UE must also be provided with the seamless application mobility.
- **Issues:**
  - Solve the issues while achieving low latency:
    - How to authenticate UE with the computational services provided by foreign cloud.
    - How to authenticate the UE with foreign cloud.
    - How to communicate between fog and cloud.

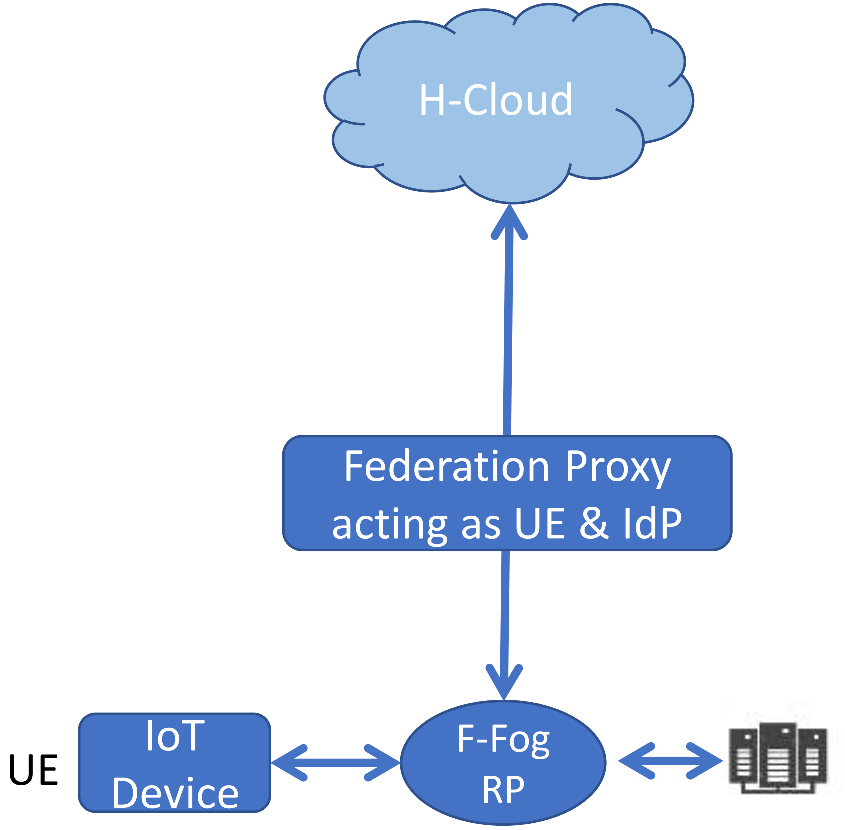
Survey

Name	Method	Problem	Scenarios	Transparent ?	Multiple Protocols?
Sarang [21]	SDN	Security	× [F-C]	× [New]	×
Kertesz [25]	MobIoT Sim	Latency	X [IoT-F-C]	X [New]	x
Souvik [26]	SFDDM	Security	X [F2C]	x	X
Tao [27]	Foud	Latency	X [V2G]	--	x

Proposed Solution

- Federation proxy between cloud and fog
- Roles have been defined for federation proxy [F-C and C-F]
- Message flow has been designed for:
    - Federated Authentication

Proposed Solution-I



H-Cloud

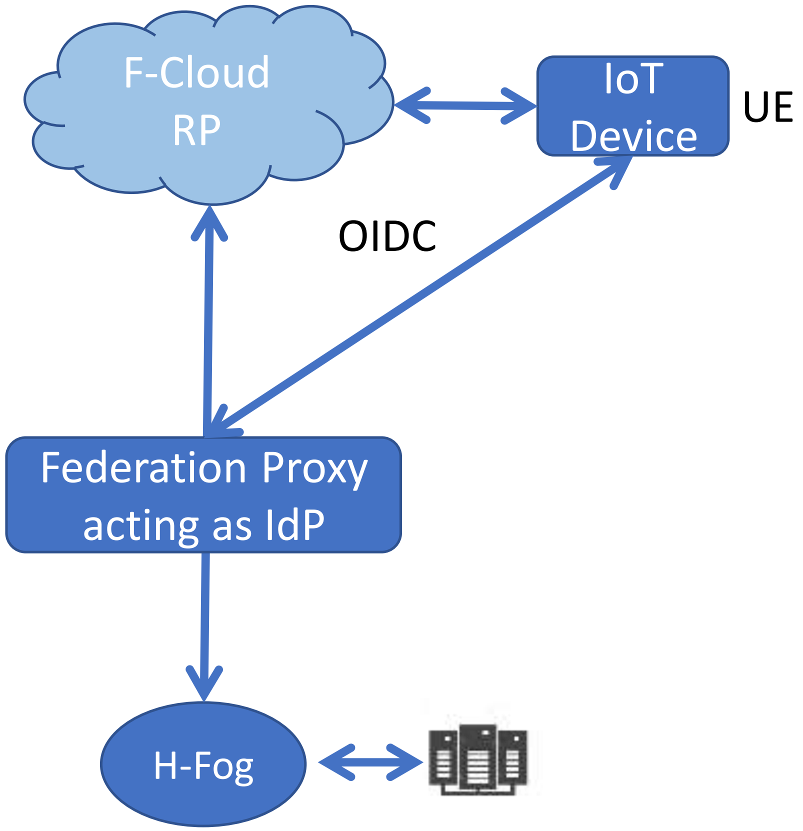
Federation Proxy acting as UE & IdP

UE

IoT Device

F-Fog RP

C-F Scenario



F-Cloud RP

IoT Device

UE

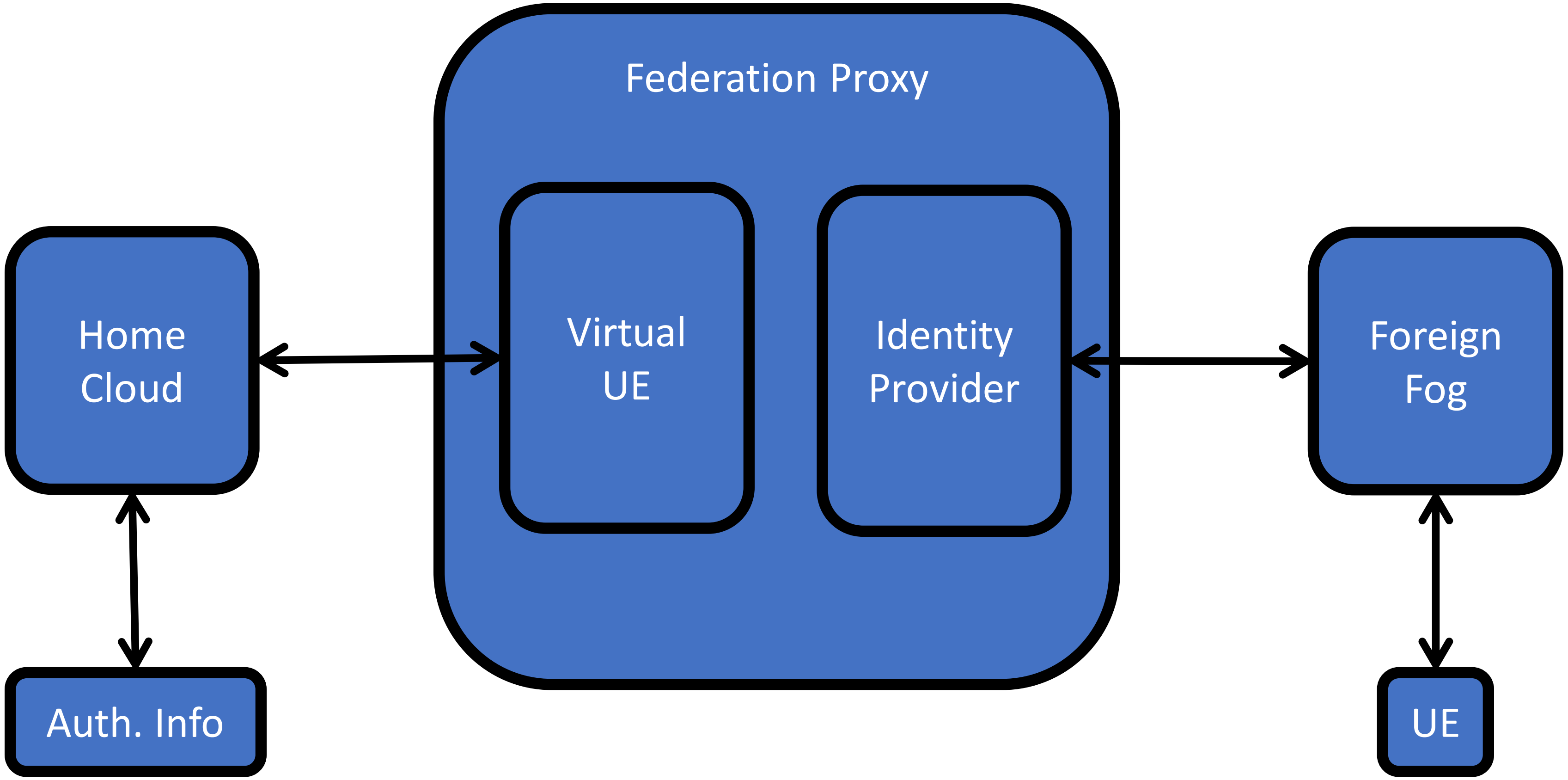
OIDC

Federation Proxy acting as IdP

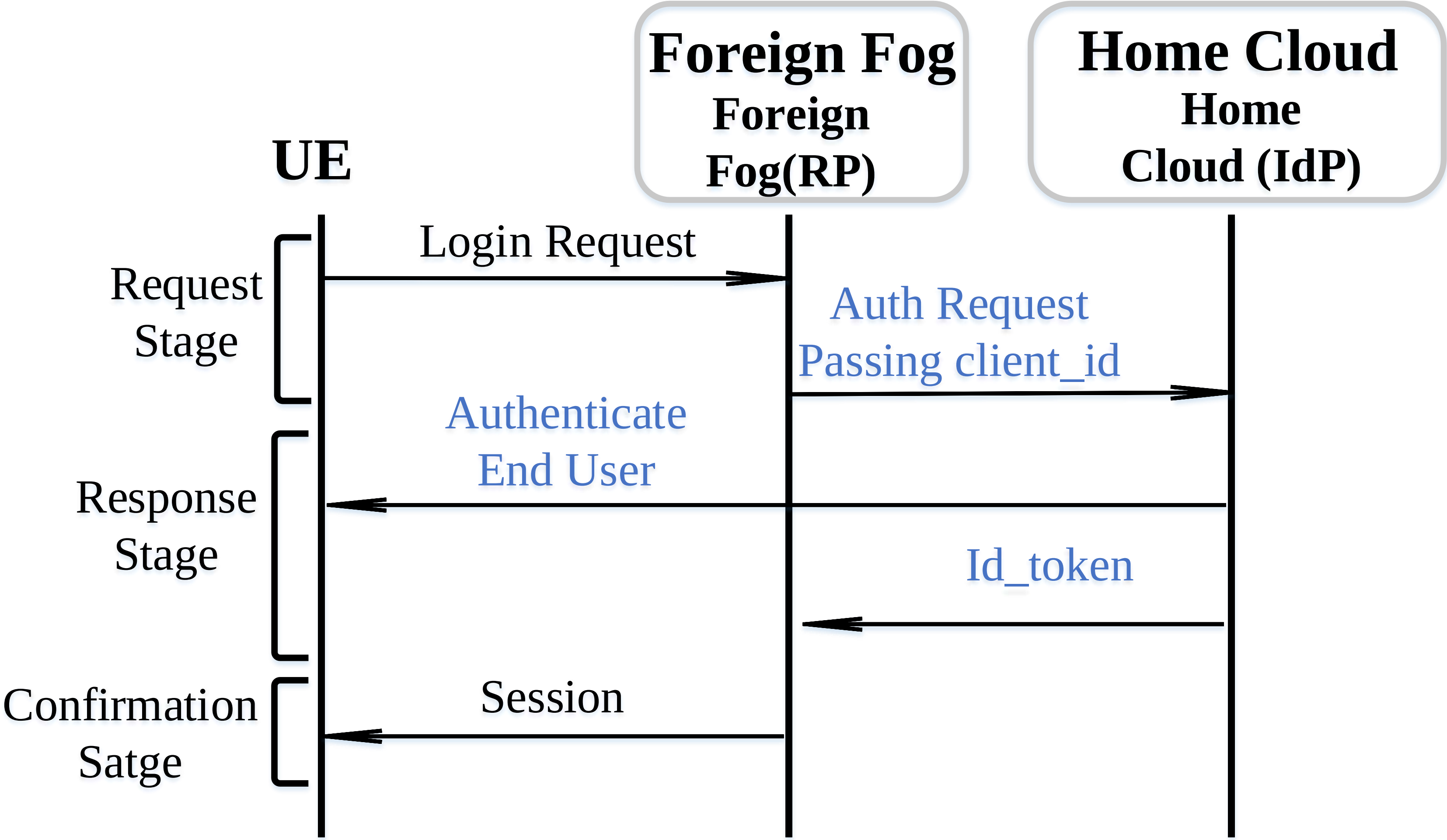
H-Fog

F-C Scenario

Proposed Solution-II [C-F Scenario]:

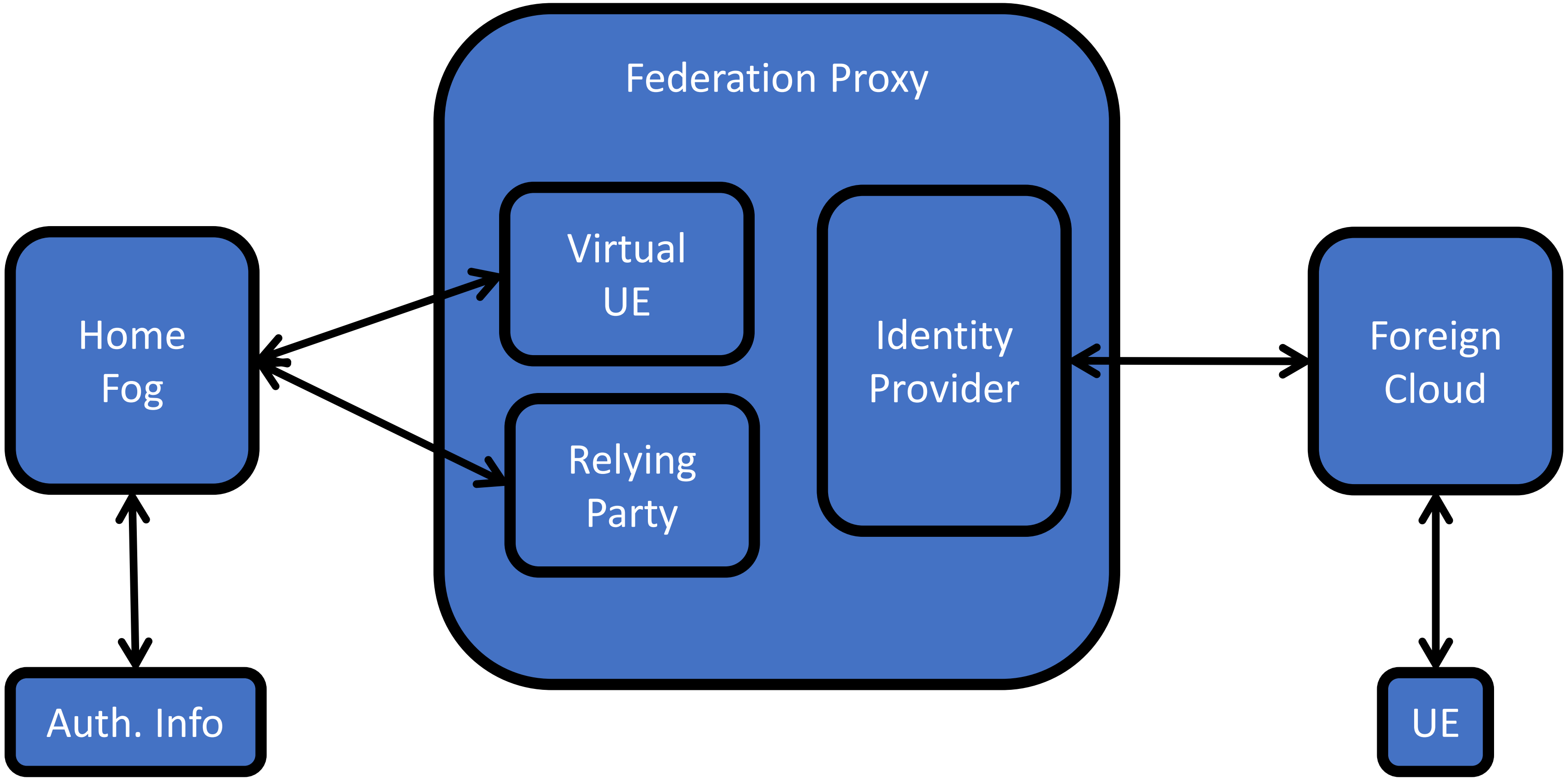


Proposed Solution-III [C-F Scenario]

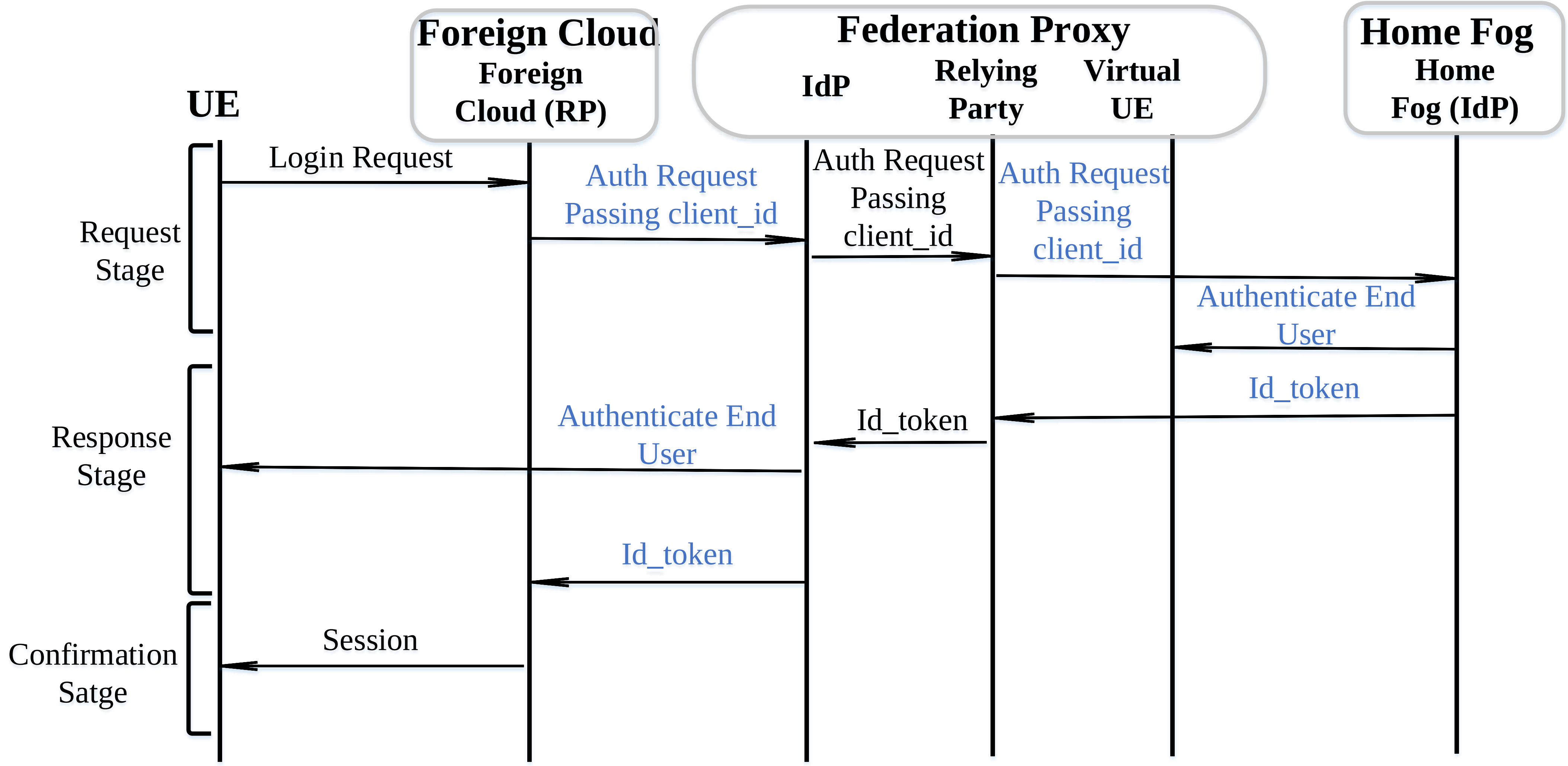


Kindly read notes for this solution

Proposed Solution-IV [F-C Scenario]:



Proposed Solution-V [F-C Scenario]

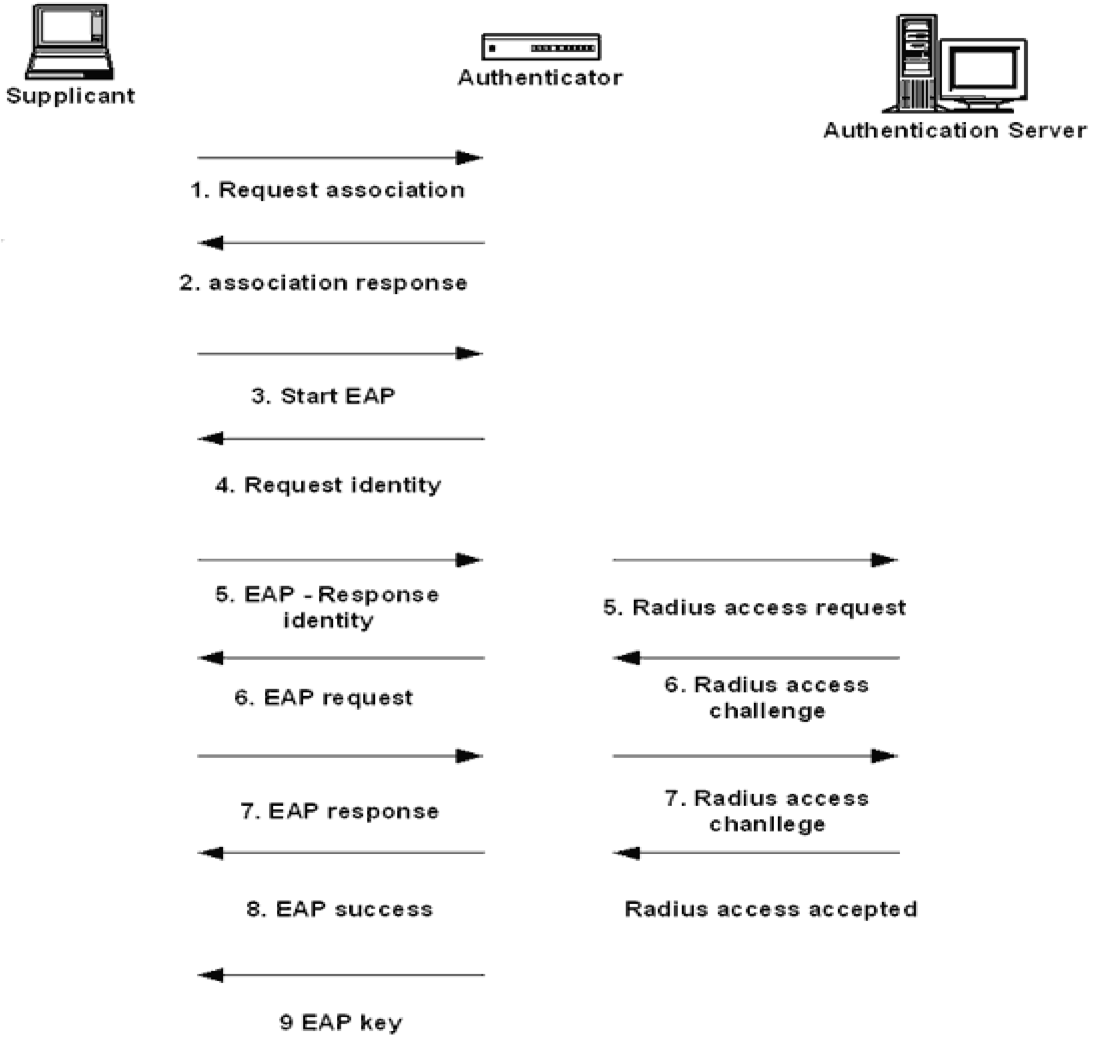


Proposed Solution V: Application Handover

- Two cases:
  - The user is a subscriber of Cloud or Fog and wants to access another a different application in Fog or Cloud.
  - The user was using a an application in Cloud or Fog and moves out of range and wants to use the exact same service from fog or Cloud
    - More likely for the Fog-to-Cloud case
    - Less likely for Cloud-to-Fog case
- The solution is through the use of Session State Token
  - TC3A
  - TS3A

Another tentative solution:802.1x

- Another tentative solution is 802.1x
- Protocol for fog devices
- Incase we can't use OIDC:
- Design message flow between
  - 802.1x for fog
  - OIDC for cloud



The important things to read

- Must understand the working of OIDC
- Must understand the working of 802.1x
- Must understand the state transfer

Further research streams following the C-F

Scenario	Federation	Federation Category	Federation Reason	Protocol Category	ID Location
1	Cloud-Fog-Fog	2-Tier one-to-many Vertical-ID upper tier	Latency/ Privacy	E	Cloud
2	Cloud-Fog-Fog	2-Tier one-to-many Vertical-ID lower tier	Capability/ Capacity	E	Fog
3	Cloud-Fog-Cloud	2-Tier many-to-one Vertical	Latency/ Privacy	E	Cloud
4	Cloud-Cloud-Fog	2-Tier Hybrid-ID upper tier	Capability/ Privacy	A, E	Cloud
5	Cloud-Cloud-Fog-Fog	2-Tier Hybrid-ID lower tier	Capability/ Capacity	A, E	Fog

References

- [1] https://telecomreseller.com/2018/02/20/ cloud-computing-vs-fog-computing-storing-your-companys-data/
- [2] Leandro, Marcos AP, et al. "Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth." Proceedings of the Eleventh International Conference on Networks. 2012.
- [3] Celesti, Antonio, et al. "Security and cloud computing: Intercloud identity management infrastructure." Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on. IEEE, 2010.
- [4] Celesti, Antonio, et al. "Three-phase cross-cloud federation model: The cloud sso authentication." Advances in Future Internet (AFIN), 2010 second international conference on. IEEE, 2010.
- [5] Ahmad, Zubair, Jamalul-Lail Ab Manan, and Suziah Sulaiman. "User requirement model for federated identities threats." Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on. Vol. 6. IEEE, 2010.
- [6] Yan, Liang, Chunming Rong, and Gansen Zhao. "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography." IEEE International Conference on Cloud Computing. Springer, Berlin, Heidelberg, 2009.
- [7] Stihler, Maicon, et al. "Integral federated identity management for cloud computing." New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on. IEEE, 2012
- [8] A. Donald, L. Arockiam, A Secure Authentication Scheme for MobiCloud, in: International Conference on Computer Communication and Informatics (ICCCI), 2015, pp. 1–6.

References

- [9] M. H. Ibrahim, Octopus: An Edge-fog Mutual Authentication Scheme, International Journal of Network Security 18 (6) (2016) 1089–1101
- [10] S. Xu, E. P. Ratazzi, W. Du, Security Architecture for Federated Mobile Cloud Computing, in: Mobile Cloud Security, Springer, 2016
- [11] S. Bouzefrane, A. Benkara Mostefa, F. Houacine, H. Cagnon, Cloudlets Authentication in NFC-Based Mobile Computing, in: Proceedings of the 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014, pp. 267–272.
- [12] Lai, Chengzhe, et al. "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks." *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014.
- [13] Imine, Youcef, et al. "MASFOG: An Efficient Mutual Authentication Scheme for Fog Computing Architecture." *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018.
- [14] Amor, Arij Ben, Mohamed Abid, and Aref Meddeb. "A Privacy-Preserving Authentication Scheme in an Edge-Fog Environment." *Computer Systems and Applications (AICCSA), 2017 IEEE/ACS 14th International Conference on*. IEEE, 2017.
- [15] Al Shidhani, Ali A., and Victor CM Leung. "Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers." *IEEE transactions on dependable and secure computing* 8.5 (2011): 699-713.
- [16] Chen, Yu-Chang, Ja-Hsing Hsia, and Yi-Ju Liao. "Advanced seamless vertical handoff architecture for WiMAX and WiFi heterogeneous networks with QoS guarantees." *Computer Communications* 32.2 (2009): 281-293.

References

- [17] Mun, Hyeran, Kyusuk Han, and Kwangjo Kim. "3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA." 2009 Wireless Telecommunications Symposium, WTS 2009. IEEE, 2009.
- [18] Shi, Minghui, et al. "A service-agent-based roaming architecture for WLAN/cellular integrated networks." *IEEE Transactions on Vehicular Technology* 56.5 (2007): 3168-3181.
- [19] Jiang, Yixin, et al. "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks." IEEE Transactions on wireless communications 5.9 (2006): 2569-2577.
- [20] Shi, Minghui, Xuemin Shen, and Jon W. Mark. "IEEE 802.11 roaming and authentication in wireless LAN/cellular mobile networks." IEEE Wireless Communications 11.4 (2004): 66-75.
- [21] Kahvazadeh, Sarang, et al. "Securing combined fog-to-cloud system through SDN approach." *Proceedings of the 4th Workshop on CrossCloud Infrastructures & Platforms*. ACM, 2017.
- [22] Targali, Yousif, Vinod Choyi, and Yogendra Shah. "Seamless authentication and mobility across heterogeneous networks using federated identity systems." 2013 IEEE International Conference on Communications Workshops (ICC). IEEE, 2013.
- [23] Choyi, Vinod K., and Alex Brusilovsky. "Seamless authentication across multiple entities." U.S. Patent Application No. 14/779,584.
- [24] Mwangama, Joyce, et al. "Towards mobile federated network operators." Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft). IEEE, 2015.
- [25] Kertesz, A., T. Pflanzner, and T. Gyimothy. "A mobile IoT device simulator for IoT-Fog-Cloud systems." Journal of Grid Computing 17.3 (2019): 529-551.

References

- [26] Sengupta, Souvik, et al. "SFDDM: A Secure Distributed Database Management in Combined Fog-to-Cloud Systems." 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE, 2019.
- [27] Tao, Ming, Kaoru Ota, and Mianxiong Dong. "Foud: Integrating fog and cloud for 5G-enabled V2G networks." IEEE Network 31.2 (2017): 8-13.