IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 9, 2022, accepted March 20, 2022, date of publication March 28, 2022, date of current version April 5, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3162851

Federated 3GPP Mobile Edge Computing Systems: A Transparent Proxy for Third Party Authentication With Application Mobility Support

ASAD ALI[1], (Graduate Student Member, IEEE), SAMIN RAHMAN KHAN[2], SADMAN SAKIB[2], MD. SHOHRAB HOSSAIN[2], (Member, IEEE), AND YING-DAR LIN[1], (Fellow, IEEE)

[1]Department of Computer Science, National Yang Ming Chiao Tung University, Hsinchu 300, Taiwan
[2]Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology, Dhaka 1000, Bangladesh

Corresponding author: Samin Rahman Khan (saminrahmankhan97@gmail.com)

This work was supported by the Ministry of Science and Technology, Taiwan, under Project 108-2221-E-009-046-MY2.

ABSTRACT Multi-Access or Mobile Edge Computing (MEC) is being deployed by 4G/5G operators to provide computational services at lower latencies. Federating MECs across operators expands capability, capacity, and coverage but gives rise to two issues for continuous service during roaming without re-authentication—third-party authentication and application mobility. In this work, we propose a Federated State transfer and 3rd-party Authentication (FS3A) mechanism that uses a transparent proxy to transfer the information of both authentication and application state across operators to resolve these issues. The FS3A proxy is kept transparent with virtual counterparts to avoid any changes to existing MEC and cellular architectures. FS3A provides users with a token which, when authenticated by an MEC, can be reused across operators for faster authentication. Prefetching of subscription and state is also proposed to further reduce authentication and application mobility latencies. We evaluated FS3A on an OpenAirInterface (OAI)-based testbed and the results show that token reuse and subscription prefetching reduce the authentication latency by 53–65%, compared to complete re-authentication, while state prefetching reduces application mobility latency by 51–91%, compared to no prefetching. Overall, FS3A reduces the service interruption time by 33%, compared to no token reuse and prefetching.

INDEX TERMS Mobile edge computing, multi-access edge computing, authentication, mobility, latency, 3GPP cellular networks.

I. INTRODUCTION

Edge Computing is the computing paradigm where computation and data storage services are brought to the edge of a network, closer to its users [1]. Multi-Access or Mobile Edge Computing (MEC) is a concept that integrates computational capability with cellular networks and brings enhanced computational power closer to users [2] in order to reduce latency and bandwidth requirements and increase the quality of service. Real time applications like augmented reality, online gaming, video conferencing, video processing for autonomous vehicles etc., benefit considerably from low latency edge systems.

As the Internet of Things (IoT) continues to grow, a large number of mobile IoT devices will turn to Edge Computing and Mobile Edge computing for computation capability and networking [3]. Third Generation Partnership Project (3GPP) networks like 4G Long Term Evolution (LTE) or 5G provide the connectivity backbone for MEC. Mobile Network Operators (MNOs) can easily incorporate MEC into their existing infrastructure and provide services to their users [4]. The European Telecommunications Standards Institute (ETSI) has provided many new use cases for MEC and has pointed out that the deployment of MEC will introduce new revenue streams for operators, vendors and third-parties [5].

The associate editor coordinating the review of this manuscript and approving it for publication was Francisco Rafael Marques Lima.

A. FEDERATION

There are multiple MNOs in the world and they likely have their own MEC servers deployed in their infrastructure. The subscribers of these MNOs would be able to access the services provided by the deployed MEC servers. In the early deployment stage, individual MNOs may not be able to provide MEC coverage in all areas. Different MNOs would cover different areas, depending upon the location of MEC servers. A user will therefore not be able to get complete coverage and, if there is no collaboration among multiple MNOs, a subscriber would have to buy subscriptions from multiple MNOs and create multiple accounts for multiple application servers deployed in different MNOs. Furthermore, having to provide login credentials every time a user tries to access an application would greatly increase the latency and reduce a user's experience.

It would thus be more advantageous for both the service providers and their subscribers, if the service providers could form a federation between themselves. This kind of federation is already in practice for cloud service providers [6]. Such a federation would encourage MNOs to collaborate and share resources between themselves in order to provide multiple services and better coverage to all their users. Such a federation between MNOs is better compared to a federation between MNOs and cloud or fog networks because the base stations of MNOs are closer to each other. A federation between MNOs would therefore allow them to share resources and provide faster mobility to their users. Furthermore, a federation between MNOs would provide extended MEC service coverage.

The advantages of such a federation are twofold: MNOs would be able to serve more users and users will have access to continuous low latency MEC services without having to rely on cloud or fog. Users would be able to obtain MEC services from such a federation using just a single SIM card without having to buy subscriptions from different MNOs, and they would also be able to switch between networks in order to get the best services. A federated system would also open doors to more modularised services and applications that can be shared by multiple networks.

B. ISSUES AND RESEARCH QUESTIONS

1) AUTHENTICATION ISSUE

User equipment (UE) can authenticate itself with an MEC via its cellular authentication information which is stored in the cellular network it is registered with, which we refer to as the home network of the UE. Whenever an UE wants to use MEC services from any other network (referred as the foreign network), the MEC system needs to access the authentication information from the UE's home network in order to verify its identity. The issue that arises here is that the authentication information of the UE is kept private in the home network and is not shared outside that network's trust domain. Providing interfaces to expose the authentication information outside the cellular network would demand changes in the already established cellular network architecture and protocols. This gives rise to the third-party authentication issue where we need a mechanism by means of which the UE (first party) could authenticate itself with the foreign MEC (third party) via its home MEC (second party).

2) APPLICATION MOBILITY ISSUE

When an UE moves out of the MEC coverage of the home network, and becomes authenticated with the foreign network, we are faced with another issue that we refer to as the application mobility issue. This issue is that the UE was getting services from the MEC of the home network and now it has moved to a foreign network where it needs to get the services from the MEC platform of that network without discontinuation. If a user cannot move instantaneously into the MEC coverage of neighboring edge networks, a discontinuation of services would occur, causing the UE to fall back to the cloud servers which would, in turn, add latency and degrade the user's experience. Moreover, whenever a user switches edge networks, active application sessions must be retained because the user's convenience will be greatly compromised if the user has to login to a new network and start the session anew. The application state should remain intact and latency during transfer should also be kept to a minimum. Therefore, an MEC platform in one network needs to be able to access the user application state from other MEC platform in another network. This is the application mobility issue and we need a mechanism to transfer the user session state from one MEC to another MEC located within different networks.

3) RESEARCH QUESTIONS

In summary, we have identified two main issues for the federated 3GPP MEC systems: 3rd party authentication and application mobility. In this work, our goal is to answer to the following question: how do we support low latency MEC application authentication and mobility in a federation between multiple 3GPP MEC systems while maintaining transparency? In order to solve the identified issues, we need an intermediary body that can facilitate internetwork MEC communication, third-party authentication, and state transfer. All this has to be done while maintaining transparency and conforming to the guidelines provided by the ETSI. To come up with a transparent solution, we first look at 3GPP and ETSI standards. ETSI has provided some design specifications for MEC architecture [7], security, authentication, application mobility [8], [9], and others. We consider these specifications while proposing the solution to the identified issues.

C. TRANSPARENT PROXY SOLUTION AND LATENCY REDUCTION OPTIMIZATIONS

We have explored the literature that addresses authentication and application mobility issues in federated mobile networks. To the best of our knowledge, no recent study provides solutions to both the issues identified in the previous section. There are two different ways to solve the issues we have

identified: one is a new protocol that provides authentication and application mobility across multiple MNOs and the other is to use existing 3GPP standard protocols and construct a solution using existing protocols. The latter is preferable as it does not involve any modifications of existing protocols and provides transparency.

Various solutions have been proposed for developing a transparent, low latency system that provides Authentication, Authorization, and Accounting (AAA) functionality in a MEC system in a single network [10]. Transparent solutions have also been proposed for third-party authentication and application mobility between MEC platforms in a single network [11]. Our proposal integrates these to provide a solution to authentication and application mobility problems in federated 3GPP inter-MNO MECs, is transparent, and meets the low latency requirements in a federated 3GPP MEC System.

We propose an FS3A mechanism that makes use of a transparent proxy that can transfer authentication and application state information across the MNOs to provide 3rd-party authentication and application mobility. The basic idea is based on a proxy network that keeps inter-MNO communications close to the ground and leverages roaming-based cellular authentication to provide 3rd party application authentication in foreign networks. The proxy consists of virtual counterparts, so as to avoid any changes to the existing MEC and 4G/5G cellular network architectures. UEs are authenticated by a foreign MEC network by inspecting cellular traffic during roaming authentication in the foreign cellular network. The MEC network can then provide access tokens to the UEs for accessing its application servers. FS3A also provides scope for reusing application access tokens across the MECs that belong to other MNOs for faster authentication. In FS3A, an MEC-tier application state transfer is carried out using MEC host and system-level entities to manage the application mobility in the federation. Subscription data and application state data prefetching are done to further reduce the authentication and application mobility latencies. The main contributions of this work are summarized as follows:

- We propose a federation between MECs deployed by different MNOs and develop an FS3A mechanism for solving the third-party authentication and application mobility issues in the proposed federation.
- The FS3A makes use of a proxy network, host and system level MEC entities to transfer the authentication and application state information across MECs in different MNOs. These adaptations are compliant with current MEC specifications, existing 4G LTE network standards and will be compatible with 5G standards as well.
- FS3A demonstrates how low-latency application authentication is provided in foreign MEC systems by inspecting roaming cellular authentication. FS3A provides scope for reusing application access token without re-authentication through MEC system, reducing application down-time while moving across networks.

TABLE 1. Abbreviations and their meaning.

Abbreviations	Meaning
3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
AMC	Application Mobility Coordinator
AMS	Application Mobility Service
eNB	eNodeB
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FS3A	Federated State transfer and 3rd-party Authentication
HSS	Home Subscriber Server
MEC	Mobile Edge Computing
MEO	MEC Orchestrator
MME	Mobility Management Entity
MNO	Mobile Network Operators
OAI	OpenAirInterface
SPGW	Serving and Packet Gateway
TC3A	Token-based Cookie transfer & 3rd-party Authentication
TS3A	Token-based State transfer & 3rd-party Authentication
UE	User Equipment

- FS3A carries out subscription data and application state data prefetching to further reduce the authentication and application mobility latency.

The rest of the paper is organised as follows. In Section 2, we review the 3GPP and ETSI standards, provide the threat model for our problem and explore relevant literature to learn how similar problems were solved. In Section 3, we state the proposal and provide some examples to illustrate various scenarios, and in Section 4 we described in detail our approach, architecture design, and message flows. Section 5 details the implementation, modules, and testbed. Section 6 reflects the results and evaluation, and we conclude the paper in Section 7 and present some issues to be investigated in the future.

II. BACKGROUND AND RELATED WORK

In this section we discuss existing 4G LTE architecture with MEC, some of the relevant ETSI MEC standards, a threat model for our problem, and related work. Abbreviations used in this paper are listed in Table 1.

A. EXISTING 4G-LTE ARCHITECTURE WITH MEC

4G-LTE is the most widespread mobile network in the world and is a prime candidate for an underlying cellular network within which MEC systems will function. Designs developed for an LTE network will also have to be compatible with future 5G networks. An UE, eNodeB (eNB), and an Evolved Packet Core (EPC) constitute an LTE system. EPC consists of a Home Subscriber Server (HSS), Mobility Management Entity (MME), and Serving and Packet Gateway (SPGW). An UE is the end-device through which a user communicates with an EPC via eNB. The HSS acts as the database of all cellular information of subscribers. The MME manages the access and mobility aspects of each UE. MEC servers can be

deployed in 4G LTE network through different architectures provided by ETSI [12]. In order to achieve lower latency, we used the Bump-in-the-wire approach where the MEC platforms are deployed in between the eNBs and the EPC.

B. MEC ENTITIES AND ETSI STANDARDS FOR MEC

An MEC system consists of different host- and system-level entities which manage the functionalities within a single MEC platform, and the functionalities across all the platforms in the system. The MEC manager is a host level entity that manages the components inside the MEC platform. An MEC Orchestrator (MEO) is a system-level entity that maintains an overview of the MEC system based on deployed mobile edge hosts, available resources, available mobile edge services, and topology. An MEO also triggers application instantiation, termination, and application relocation at different MEC platforms in order to provide the best services based on the available resources [9]. As per ETSI standards, application mobility services are to be provided by MEC systems. MEC systems also need to provide information necessary for MEC applications about when and where to transfer user context during application mobility [13]. This overview of the MEC system explains the functionality of different components and helps to identify how the functionality of these components can be extended to accommodate federated authentication and mobility.

C. THREAT MODEL

In this work a cellular network and an MEC system are considered benign. UEs are, however, considered to be malicious, and a malicious UE may or may not be a user of the underlying cellular network. Malicious traffic sent by UEs can be handled by the core of an LTE network, but since MEC traffic does not go through the core network, malicious UEs can pose different threats to MEC systems. A malicious user may steal user IDs from other users or may reuse an ID that has already been used by itself or by others to obtain unauthorized access to MECs. Users may also hijack session IDs of others and may generate large amounts of traffic to incapacitate an MEC system. A federated MEC system should be resilient against such attacks. In section 4, we will see how our design copes with these problems.

D. RELATED WORK

In order to find solutions to the problem we have posed, we reviewed studies that have proposed solutions to at least one of these problems, either 3rd party authentication in federated systems, multi-network authentications, or application mobility across networks. We analyzed the transparency of these proposals according to existing LTE protocols and MEC standards. Our findings are summarized in Table 2. Donald and Arockiam [14] propose third-party authentication through the cloud. There are also studies [15]–[19] that use blockchain, mutual key exchanges, Reinforcement learning (RL), and federated IDs to manage Multi-network authentication. Han *et al.* [20] provide handover authentication by improving the existing EAP-AKA protocol and Niewolski *et al.* [21] makes use of tokens to provide service access control in 5G MEC. A few studies [22], [23] also use SDNs to manage authentication and application mobility in federated networks, while Pencheva *et al.* [24] provides application driven handover while retaining transparency.

We also looked into studies that propose solutions for application relocation, and most of these focus on VM migration, for example [25] and [26]. On the other hand, recent papers also provides transparent, low-latency solutions for authentication and mobility within a single edge network [11], [27][28], anonymous mutual authentication in MEC platforms [29], and third-party authentication between cloud and edge [30]. Some work has also been done on the deployment of a secure MEC system in a cellular network that can itself provide authentication for its applications [10]. We use this MEC deployment method in our work and extend it further across federated MNOs.

An earlier paper of ours [11] provides low latency authentication and state transfer while moving from one MEC platform to another by using two approaches, termed Token-based Cookie transfer & 3rd-party Authentication (TC3A) and Token-based State transfer & 3rd-party Authentication (TS3A). In order to compare this work with [11], we summarize the differences in Table 3. It can be seen that TC3A, TS3A, and our proposed FS3A provide third-party authentication and application mobility, but FS3A does this in a federated MEC system. The major advantage of FS3A over TS3A and TC3A is that it solves the problems of subscription and state data prefetching and provides Inter-MNO MEC connectivity, while TS3A and TC3A work for Intra-MNO MECs that are deployed by the same MNO.

Our survey shows that previous studies have provided solution to authentication and application mobility issues independently in the MECs deployed by an MNO but, none has proposed solutions for authentication and application mobility issues while maintaining the transparency and latency requirements in federated MEC systems across multiple MNOs. It should be noted that we do not try to solve the call and data roaming problems as they have already been addressed by various studies [31], [32] [33]. We focus solely on solving the problems of third party authentication and application mobility for a user that roams between MECs deployed by different MNOs. To the best of our knowledge, ours is the first work that provides a complete solution to the problems at hand, i.e., third-party authentication and application mobility in federated MEC systems, while meeting transparency and latency requirements. We adopt the transparent, low-latency authentication solutions from Intra-MNO MEC [10], [11] and enhance them to solve the problem of third-party authentication and state transfer in an Inter-MNO MEC federation.

III. PROBLEM STATEMENT

Low latency third-party authentication and application mobility in a federated MEC system are the two problems we aim

TABLE 2. Related work.

Author	Method	3p/Multi-Network Authentication	Application Mobility	Transparency
Donald [14]	Mobile Cloud Authentication	✓	X	✓
Bonnah [15]	Decentralised Blockchain Infrastructure	✓	X	X
Targali [16]	Mutual Key Exchange	✓	X	X
Choyi [17]	Authentication Proxy	✓	X	X
Edris [18]	Federated ID, Oauth2	✓	X	X
Cui [19]	Reinforcement Learning	✓	X	✓
Han [20]	Handover Authentication	✓	X	✓
Danial [22]	SDN	✓	X	X
Mwangama [23]	SDN	X	✓	X
Pencheva [24]	Application Driven Handover	X	✓	✓
Ours	Transparent Proxy	✓	✓	✓

TABLE 3. TC3A, TS3A, and FS3A comparison.

Parameters	TC3A	TS3A	FS3A
3-p Authentication	✓	✓	✓
Application Mobility	✓	✓	✓
State Prefetching	X	✓	✓
Subscription data prefetching	X	X	✓
Inter-MNO Connectivity	X	X	✓

to solve. In this section, we elaborate these problems and state the assumptions we made, and issues related to these problems.

A. PROBLEM SCENARIOS

Consider two 4G-LTE MNOs in a federation which provide MEC services. We assume that they use an MECSec design [10] to manage authentication, authorization, and access control. We assume too that an UE is the subscriber of one of the MNOs (referred as the home network). The HSS in the home network contains the subscription, authentication, and other information about the UE. The other networks, where the UE does not have a subscription, are termed foreign networks. Here, we consider two scenarios. In the first, we assume that the UE wants to access the MEC's services provided by a foreign network, and where the UE needs to get authenticated in the foreign MEC with the authentication credentials from the home network, as shown in Fig. 1(a).

In the second scenario, shown in Fig. 1(b), we assume that the UE has moved to the foreign network while using an MEC service in the home network. In this case, the foreign network derives authentication information either from the home cellular network or from the home MEC system. Application state information also needs to be carried from the application instance in the home network to its foreign counterpart. Here we will only consider the scenario where the UE moves from the home to the foreign network. Cases where the user moves from the foreign to the home network have not been considered here, because the UE is already authenticated with the home network and application mobility in such a case works the same as the home to foreign networks scenario. We have

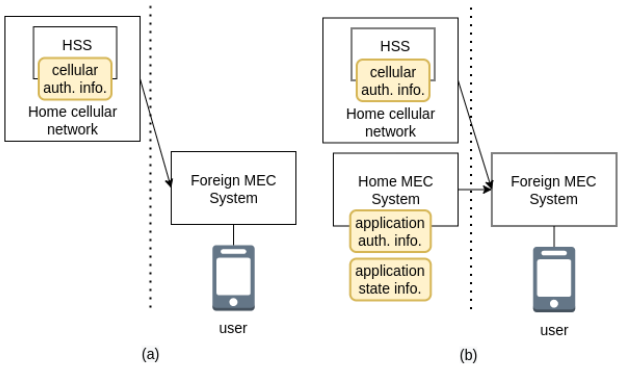


FIGURE 1. (a) Authentication problem for new application; foreign MEC system needs to authenticate UE by using cellular authentication information from the home network (b) Authentication and application mobility problems for application continuation; foreign MEC system needs to get application state from the home MEC system as well.

assumed that the underlying LTE networks are connected so as to provide roaming cellular services to their users.

B. LOW LATENCY AND TRANSPARENCY CHALLENGES

Some issues arise when an UE moves in a federated MEC system because it is important for the UE to be identified by the MEC systems in all networks by means of a common ID. The ID for each user must be unique and unchangeable. An UE is then given a unique, temporary ID by the cellular network. The entities in the cellular networks also use different temporary IDs to keep track of the tunnels formed to serve the user. The UE is also given an IP address after it has attached to the cellular network. Since the MEC platform is located between the EPC and eNBs, it can only inspect the packets in the S1 interface. An UE may come into an MEC platform either by attaching for the first time by service resumption, or via handover. In these cases, the UE attaches to the cellular networks using different IDs. Under all these circumstances, it must be ensured that the traffic from a user is uniquely identified by the MEC system.

The application mobility in MEC systems belonging to different MNOs also creates some challenges. Before the

MEC system carries out an application state transfer it must have the following information: from where the application state is to be transferred, to whom is it to be transferred, and when to carry out transfer. Since the user becomes completely detached from the home network and attaches to a foreign network, the home network has no way of determining beforehand to which foreign network the user will move, and so the MEC platform in the home MEC system cannot initiate an application handover. It is therefore important to resolve this state transfer challenge with the lowest possible latency. Another major issue is to keep the system design transparent so that no modification of the current cellular and MEC infrastructure is required. *In summary, our objective is to provide transparent 3rd-party authentication for the UEs in foreign networks along with seamless application mobility with minimal latency.*

IV. PROPOSED SOLUTION AND ARCHITECTURE DESIGN

In order to address the third-party authentication and application mobility problems identified in the previous section, along with the low latency and transparency issues, we propose FS3A mechanism.

A. FS3A

The FS3A has two parts, one for third-party authentication and one for application mobility via state transfer. For authentication in a foreign network, an MEC system picks up UE authentication information from the underlying cellular network. FS3A uses a transparent proxy in order to transfer the authentication and application state information of the UE across MECs in different MNOs. The main design idea for the proxy is transparency, and the reason behind the transparent proxy is to avoid any changes in the existing infrastructure of the underlying MEC and cellular architectures. In order to provide transparency, we propose virtual counterparts in the proxy so that the entities from the cellular and MEC systems communicate with their virtual counterparts in the proxy. The FS3A also provides the UEs with a token when they become authenticated by an MEC, which is reused across the MECs deployed by different operators for faster authentication. FS3A also makes use of subscription and state data prefetching to further reduce the authentication and application mobility latencies. For application mobility via state transfer, we included two mobility functions, the host level Application Mobility Service (AMS) and the system level Application Mobility Coordinator (AMC) in the MEC system. AMCs exchange user context and state transfer information through the proxy that provides the means for inter-MNO communication.

FS3A places most of the responsibility of application state transfer on the mobility management functions (AMS and AMC) which reduces the burden on the MEC applications and UEs. FS3A does not require any assistance or intervention from the user, making it highly secure and fast as all the processes are run in the MEC tier. The proposed FS3A solution also makes use of a few optimizations such as the token reuse instead of re-authentication at the foreign network and data prefetching in order to further reduce the latency. Overall, FS3A is transparent in design, fast, and secure from the attacks of malicious users, and it is also easy to deploy. The proposed proxy-based solution is unique as it not only provides the solutions for third-party authentication and application mobility issues in federated 3GPP inter-MNO MECs, but also provides (subscription and state) data prefetching and token reuse to reduce the latency. In the next section, we look in more detail at the architecture design and individual components that are required for FS3A.

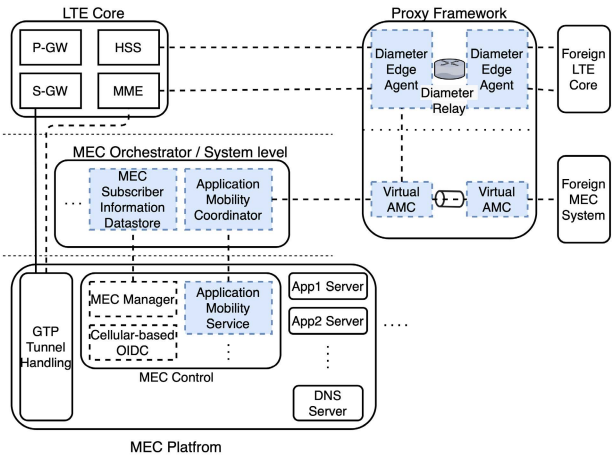


FIGURE 2. Architecture design of a MEC system in the federation. (The entities highlighted in blue are the ones we have added or extended in our proposed solution.)

B. ARCHITECTURE

FS3A provides MEC-tier authentication and state transfer via a transparent proxy. The following components have been added or extended in the MEC system to accommodate FS3A: a system-wide datastore for each MEC system and mobility functional components, host-level AMC, and system level AMS (Fig. 2). The proxy system consists of distributed, interconnected proxy entities through which MEC systems and their underlying cellular networks connect to foreign networks via virtual counterparts, so that the transparency is maintained. The MME and HSS communicate through a S6a interface which uses the Diameter protocol. In the MEC domain, virtual AMCs transfer messages related to user context from one network to another. To route the messages, the virtual AMCs have tables which store routing information for each of the networks.

1) MEC MANAGER AND MEO

The MEC Manager and cellular-based OIDC module work according to MECSec design [10] with some additional functionalities for our federated design. The MEC Manager is responsible for the activation and deactivation of MEC service for each UE. It fetches UE's cellular credentials/attributes (IP, TEID, IMSI, subscription info etc.)

from the associated LTE network or UE's home network. A system-wide datastore for each individual MEC system was added for storing all authentication information and user information, making it possible for the MEC system to store and share user information among MEC host platforms during its lifetime in the network. The MEC subscriber datastore is a distributed database system placed inside each network and is used for storing and sharing identity and other UE information throughout the MEC system. The datastore is They are incorporated along with the Mobile Edge Orchestrator (MEO) of the MEC system. The data are indexed with the most frequently used IDs. The data of UEs are kept in datastores near the UE's location. These strategies allow for quicker access times.

2) AMS AND AMC

The Application Mobility Service, or AMS, is the host level mobility function which exposes an interface with the MEC applications. The interfaces are provided by the applications for fetching the latest state information when requested by the MEC system. It is the task of the AMS to fetch state information from those applications where the UE previously had a session, and to provide the state information to the application where the UE has now moved. The AMC transfers the state information between different MEC platforms. When the state information is sent to a different network, it is passed through the proxy. The system-level mobility functions can be added to the MEO or can be placed into a separate component. For our proposed architecture, we have assumed that the MEC platforms have followed the MECSec design and have the AAA and access control components within them.

C. MESSAGE FLOWS

The message flows for Federated 3rd-party authentication and state transfer in the FS3A procedure are elaborated below.

1) 3rd-PARTY AUTHENTICATION

Third party authentication for a foreign MEC application occurs in two stages, an UE identification stage and an application authentication stage.

a: UE IDENTIFICATION

UE identification at a foreign network occurs when a UE attaches to that network for the first time. When a UE attaches (step 1) to a foreign network during roaming, the authenticating MME and the home HSS are located in two different networks, and the authentication and location update messages travel across the networks through proxies. The S1 traffic between the MME and the eNB remains the same during the process, be it in a foreign or in the home network. Fig. 3 shows that the MEC manager checks the S1 control plane traffic (steps 2, 12) and checks the transferred cellular IDs during the initial attachment procedure (steps 1-7) to ascertain whether any UE from another network has attached to the eNB where the MEC platform is deployed. When an UE attaches to a

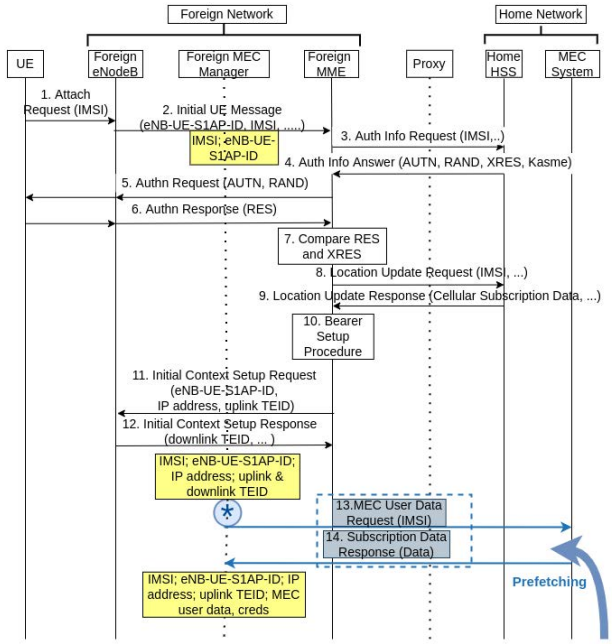


FIGURE 3. UE identification stage message flow for third-party authentication at foreign network. The star marks the stage when the foreign MEC system has confirmed the entry of UE in its network and can start pre-fetching information (both authentication and state) from its home network.

network, the MEC manager obtains the necessary ID of the UE from the S1 control plane packets, and obtains the IMSI by inspecting the Initial UE Message (step 2). The MEC manager maps the IMSI to a TEID address and an IP address by looking at the Initial Context Setup Request (step 12). The MEC manager then gathers all the necessary information about the UE in different stages as shown in Fig. 3 and stores them in the subscriber datastore.

b: APPLICATION AUTHENTICATION

After the MEC system has identified the UE in the network, the cellular OIDC module can provide the identity of the UE to the requesting MEC application servers. The cellular OIDC modules then identify the UEs by mapping the source IP address of the authentication request packet sent by the UE with their IMSI. The authorization of a user in the MEC network is validated based on the SLA (Service Layer Agreement) of the MEC network and the information of user from the subscriber datastore. If the user has authorization to use the application, the module provides the identity to the corresponding MEC server through the OIDC process. Then the MEC Application server provides the user with an authentication token.

2) STATE TRANSFER

The state transfer portion of FS3A is also broken down into two stages, a setup stage and a handover stage. For application mobility we need the coordinated action of the AMS in the host level and the AMC in the system level.

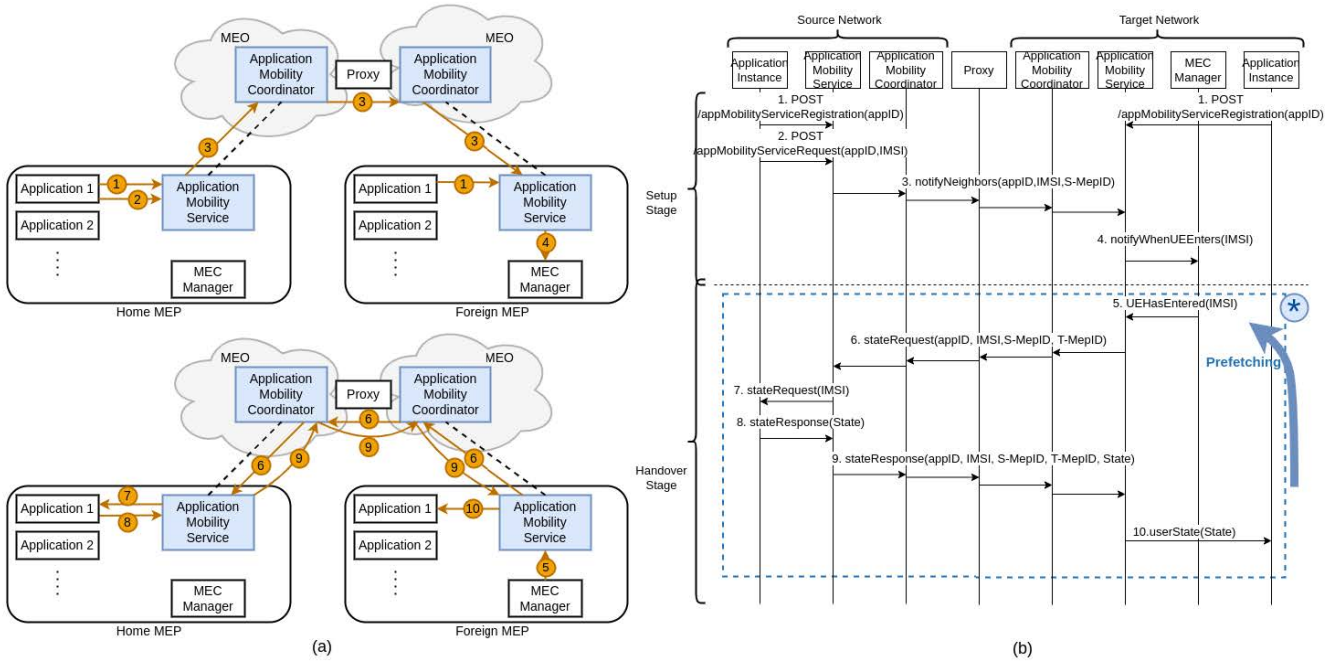


FIGURE 4. **(a) Communication between entities during FS3A state transfer: setup stage (top) and handover stage (bottom) (b) FS3A state transfer message flow. The star marks the earliest time when the foreign MEC system has confirmed UE entry and can start pre-fetching state information from its home network.**

The AMS provides an interface for the MEC applications for accessing mobility services from the MEC system. Fig. 4(a) shows the FS3A communication between different entities for application mobility and Fig. 4(b) shows the message flow.

a: SETUP STAGE

If an application wants the UE state to be transferred when the UE changes platforms, the application informs the AMS beforehand (steps 1, 2). The source AMS then informs the system level AMC that an UE in its platform may transfer an application state to a neighbouring platforms (step 3). The AMC then informs about the application and the UE to the AMSs belonging to neighbouring MEC platforms of the source platform. The AMC relay these information to MEC platforms belonging to other MEC networks through our proxy. The AMC relays this information to MEC platforms belonging to other MEC networks through our proxy. A pre-configured agreement between participating MEC networks determine if and which of the AMSs of the neighbouring MEC networks are notified. In the next step, the IMSI, application Id and the source MEC Platform (MEP) ID is sent from the source AMS to the neighbouring AMSs (Step 3). Thus, the required neighbouring AMSs are informed about the source MEC Platform in which the state of application (with the application ID) for the user with the IMSI resides. This information is stored by the target AMS. When that UE enters any of those MEC platforms, they can then obtain its application state from the home MEC platform. The AMS requests the MEC Manager to notify it when a UE enters the MEC platform by providing the IMSI (step 4). The MEC Manager will inform the AMS as soon as the UE with the corresponding IMSI has entered as is authenticated, and state handover can proceed.

b: HANDOVER STAGE

When the UE enters any of the neighbouring MEC platforms, the MEC manager informs its AMS (step 5). After being informed by the MEC manager about the arrival of a user in the network, the AMS fetches its application state from the source MEC platform. The request is relayed from the target AMS to the source AMS through the higher-tier AMCs and proxy (Step 6). The request contains the Application Id, IMSI and MEP IDs of the source and target platforms. The source AMS then requests the application state of the user with the IMSI from the application server with the application Id (Step 7). This request contains the IMSI of the UE. The application server responds with the latest application state of the UE (Step 8), which is then relayed through the AMC and the proxy back to the target AMS (steps 9). This response contains the application Id, IMSI and the MEC Platform IDs. After the state information reaches the AMS, it provides the information to its corresponding application (step 10). MEC-tier state transfers are more resilient to network interruptions. If partial data transfers occur during network disruptions, remaining data are re-requested by foreign MEC system from the home MEC system through the underlying, reliable

transport layer protocol. With repeated failure the user is notifies, and can then re-request data transfer at a later time.

3) OPTIMIZATIONS

The delays resulting from third-party authentication and state transfer can be reduced further with two optimization steps, prefetching and token reuse.

a: DATA PREFETCHING

The state and subscription data of a user can be transferred as soon as the target MEC manager detects that the UE has connected to its network even before the UE has set up a connection with the application. This is especially helpful when data transfer is carried out between platforms in different networks. When an UE switches to a foreign network, a substantial amount of time is spent on authentication, network bearer setup, and connecting to the application. While all these processes are being carried out, the mobility functions can transfer the state to the right network. The extra time required for state and subscription data transfer is thus negated. We refer to this as data prefetching.

In our proposed solution, the target MEC requires the user subscription data from the source MEC. Although, this can be triggered after the completion of the setup procedure, a foreign MEC manager can start prefetching such data as soon as it gets confirmation of the UE's authentication and has all the necessary information about the UE. The MEC manager maps the IMSI to a TEID address and IP address from the Initial Context Setup Request. After this stage, the MEC system has confirmed the entry of the UE into its network. This prefetching step can then be started just after the Initial Context Setup Request message in EPS-AKA, as shown in the blue box (steps 13, 14) in Fig. 3. In the state transfer solution state data is fetched from the source MEC to the target MEC after the foreign MEC Manager informs foreign AMS about the UE's arrival. The state transfer starts after third-party authentication without data prefetching optimization but, just like subscription data prefetching, state transfer can also be triggered by the foreign MEC manager as soon as it confirms the UE's authentication and has necessary UE's information. State transfer can thus be initiated just after the Initial Context Setup Request message in EPS-AKA. The state data prefetching is shown in the blue box in Fig. 4. Since the MEC system already parses S1 traffic for authentication, additional computational and memory loads for prefetching are negligible.

b: TOKEN REUSE

Cellular OIDC is used to provide long-term, secure, and reliable authentication. After authentication, cellular the OIDC module redirects the user to the MEC application with an access/ID token. This token can be stored in the user's device so that when the user switches MEC network, the token can be submitted to the foreign MEC network, thus bypassing the Cellular OIDC procedure. Reusing tokens allows us to skip over the cellular OIDC procedure, and thus reduces the delay of service resumption. The MEC applications provide services to authorized users after validating the user's context (source, home network information, etc.) obtained from the token and the MEC network's SLA. The foreign network may choose to re-authenticate the user through cellular OIDC or even deny service to the user. FS3A thus provides the option for two modes of authentication: a more secure, but slower cellular OIDC-based authentication, and a faster, but short-lived token based authentication.

4) SECURITY ANALYSIS

We assumed that the MEC platforms themselves follow the MECSec design so that they have access control systems that protect against malicious traffic. The UE is authenticated in a foreign MEC system only after it has first been authenticated by the foreign cellular network. Since the MEC system uses the source IP address of a packet to identify the user that has sent it, a malicious user may try to spoof a valid IP address to gain access to the network. This is also a threat to the underlying cellular network. The cellular network attempts to mitigate this by changing the IP address of the user from time to time, making it harder for attackers to track addresses. The MEC system keeps track of these changes by inspecting the S1 control plane messages, and is then always informed about legitimate users.

The application authentication tokens may also pose a security threat as malicious users may try to generate fake tokens or tamper with tokens, or even reuse valid tokens meant for other users. Tokens are themselves made secure since they are signed and encrypted by keys only available to the applications. The lifetime of the tokens is also very short. Again, a malicious user managing only the token cannot gain entry into an MEC system, as the MEC system will inspect the IP address and determine that it is not a legitimate user. A proxy is a separate network which cannot be accessed by outside users; it is only accessed by trusted networks over secure connections. So, malicious users cannot hack into a proxy, and overall, FS3A is resilient against malicious attacks.

V. IMPLEMENTATION

In this section we cover the design of our experimental prototype, implemented modules, and the testbed used for experimentation.

A. PROTOTYPE ARCHITECTURE

We tested our proposed solution on an OAI based 4G-LTE network. The solution is equally feasible for a 5G cellular network as it does not propose any changes to the underlying cellular network architecture. We set up two networks for the prototype, each consisting of an MEC system integrated with a LTE cellular network. To run the experiment, we set up an MEC application server in each network. The MEC applications authenticate their users through cellular OIDC, and behaved the same as any OIDC Client. The cellular OIDC Identity Provider provided IMSI information

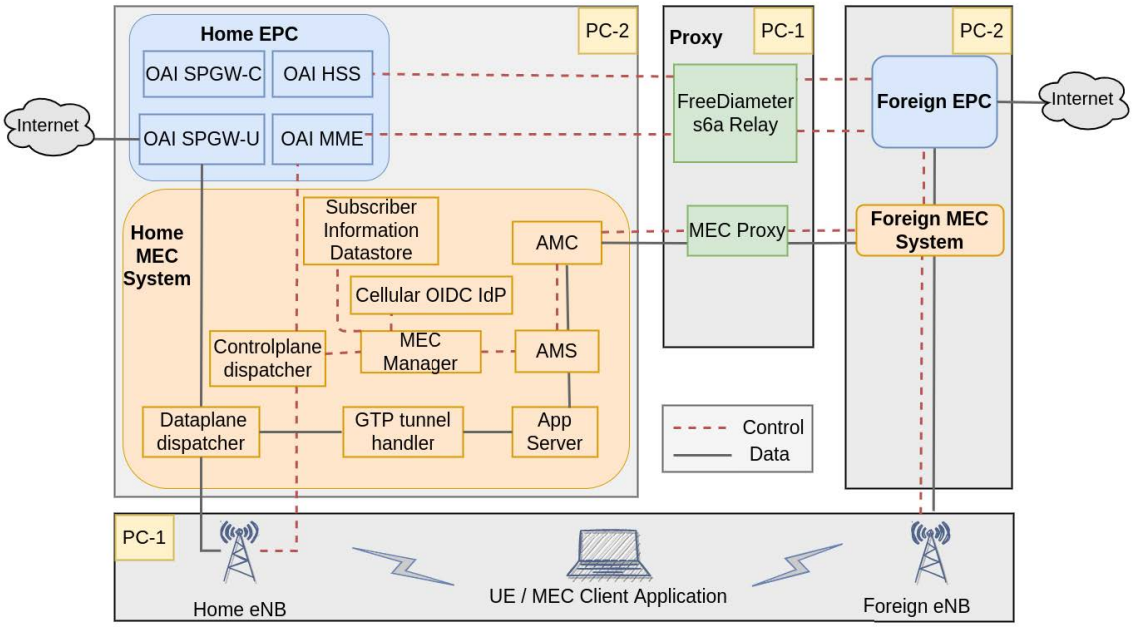


FIGURE 5. Experimental testbed.

to the MEC application as the user ID. The proxy consisted of a FreeDiameter s6a relay and a custom relay for MEC information transfer.

B. MODULES

OpenAirInterface [34] implementations provided the LTE cellular network platform. We used an ueltesimulator [35] to simulate the UE. Roaming support was added to the LTE networks so that S6a traffic of roaming users were redirected to their home networks. The dataplane dispatcher routed the MEC data towards the MEC servers and the GTP tunnelling module decapsulated the data packets before they were sent to the MEC servers. An libgtpnl library [36] was used to handle GTP tunnels. The control plane dispatcher, implemented in C, was located between the S1AP interface between the eNB and the MME and acted as a proxy, and sent a copy of the packets to the MEC Manager.

The MEC Manager was implemented with python via using the pycrate [37] library, and it parsed the messages and sent the information relevant for MEC authentication to the cellular OIDC module, which in turn accumulated them in a Dictionary. The cellular OIDC module, AMS, AMC and the MEC server application were implemented using Node.js. The front end application and back end MEC server applications were simple React and Express Node.js applications respectively. The MEC relay component of the proxy was implemented using Node.js, and the information of different networks was stored and managed by this component. They had persistent socket connections in between for faster data transfers. The detailed architecture with all the modules is shown in Fig. 5.

C. TESTBED

Our testbed was set up on 2 PCs, both with same hardware configuration and a Linux Ubuntu Operating System. The UE and eNB of both cellular networks was set up in PC-1, while PC-2 was set up with the EPC and MEC components. Proxy components were set up in PC-1 to make communication between two EPC more realistic. Docker was used to containerize the components and docker networks were used to create virtual networks in each PC. Both the PCs were connected to the same LAN (100 Mbps) through a router/switch. We also deployed the authentication server which was an OIDC IdP provider written in Node.js. The cloud components were hosted in Google Cloud Platform (GCP) in order to test the latency difference between the scenario where the authentication server was deployed in the cloud and the scenario where the authentication server was deployed in the MEC. The location of the GCP server was set at asia-southeast-1 (Singapore) which was the closest available server to the rest of the testbed in Bangladesh. The bandwidth of the network between the MEC setup and the cloud was 20Mbps.

VI. RESULTS AND EVALUATION

After implementation, we evaluated our proposed FS3A design to ascertain the time taken for UE authentication in different scenarios. We then examined the state transfer latency for different state sizes and divided the UE authentication and state transfer latency into multiple stages to determine the effectiveness of the proposed token reuse and data prefetching optimizations. Finally, we investigated the service interruption latency for the different scenarios to ascertain the overall effectiveness of FS3A.

TABLE 4. Different scenarios created via multiple combinations of Auth server location, state prefetching and token reuse.

Scenarios	Authentication Server Location	Timing for Fetching subscription data	Token Reuse or Re-authentication
CUA	Cloud(C)	During User Auth (U)	Re-authentication (A)
CUT	Cloud(C)	During User Auth (U)	Token Reuse (T)
CPA	Cloud(C)	Prefetching (P)	Re-authentication (A)
CPT	Cloud(C)	Prefetching (P)	Token Reuse (T)
MUA	MEC(M)	During User Auth (U)	Re-authentication (A)
MUT	MEC(M)	During User Auth (U)	Token Reuse (T)
MPA	MEC(M)	Prefetching (P)	Re-authentication (A)
MPT	MEC(M)	Prefetching (P)	Token Reuse (T)

A. UE AUTHENTICATION LATENCY

For the first set of results, we investigated the UE authentication latency by dividing it into three steps: authentication with the foreign MEC, access control by checking subscription data, and registration by edge application in target MEC. We also considered multiple scenarios that calculated the UE authentication latency in order to determine the efficiency of FS3A. First, OIDC authentication latency was measured as the time taken by target MEC manager to authenticate UE with the help of an OIDC Identity Provider (IdP). Access control latency was then measured as the time for MEC manager in target the MEC to collect subscription data from source the MEC to determine access to the requested service. Finally, UE registration latency was measured as the time the MEC app server took to store subscriber information in application database and to confirm UE authentication to UE client application. The authentication time was calculated for 8 possible scenarios, as shown in Table 4. We designed these scenarios by placing an OIDC IdP either in the cloud or in the MEC according to our proposals, by fetching the subscription data during UE authentication or prefetching, and by carrying out the UE re-authentication at the target MEC, or reusing the authentication token provided to the UE by the application server in the home MEC.

We calculated the UE authentication latency for all 8 scenarios (Fig. 6). It was evident that the MPT scenario (FS3A) took the least amount of time as it used the subscription data prefetching and reused the authentication tokens while the authentication server was in the MEC. The results also show that placing the authentication server in the MEC reduced the latency by 28–58%, compared to placing the authentication server in the cloud. We also found that the token reuse and the subscription data prefetching reduced the authentication latency by 53–65%, compared to the complete re-authentication and subscription data fetching during UE authentication. This clearly shows the importance of the proposed token reuse and data prefetching optimizations.

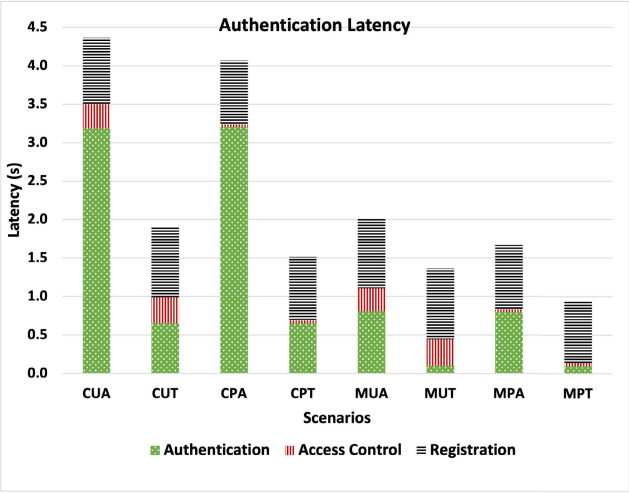


FIGURE 6. UE authentication latency.

B. STATE TRANSFER LATENCY

For the second set of results, we calculated the state transfer latency to see how much time was taken to fetch the application state from the UE's home network in order to resume the application in the target network. We measured this latency for states of different sizes in three different cases. In the first, the state was downloaded from the cloud to target MEC, which might be required if there is no FS3A in place to transfer the state from one MEC to another MEC. In the second, the state was transferred via MEC proxy without using the state data prefetching, while in the third case, state was transferred via MEC proxy along with the state data prefetching. Both MECs and cloud were set up as stated in section V.C. State transfer was requested with HTTP GET method and latency was measured as the time between requesting the state and having the complete state in target MEC App server.

Fig. 7 shows the state transfer latency comparison of the above three cases for state sizes of 10 KB, 1 MB, and 10 MB. It is clear from Fig. 7 that, as the state size increased, the latency for the state transfer via the cloud server during handover increased considerably. We therefore suggest that MNOs avoid using the cloud for state transfer as it leads to poor user experience. Our proposed FS3A (without state prefetching) took much less time compared to state transfer via the cloud, as it transferred the state via the MEC proxy. It can also be seen that, by using state prefetching, we further reduced the state transfer latency by 51.4%, 80.6% and 91.3% for state sizes of 10 KB, 1 MB, and 10 MB, respectively, compared to state transfer without prefetching. On average,

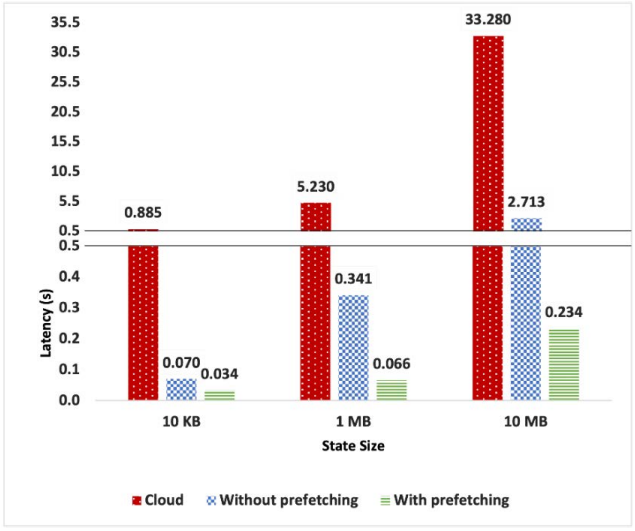


FIGURE 7. State transfer latency.

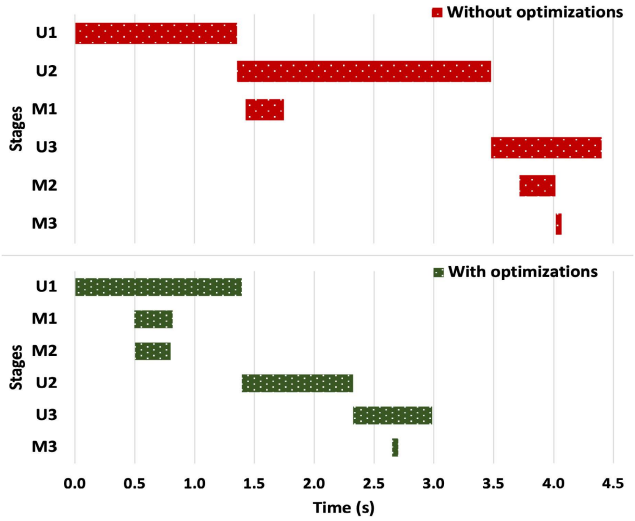


FIGURE 8. Latency breakdown with vs. without optimizations.

FS3A reduced state transfer latency by 74.4% and 98.1% compared to state transfer without prefetching and state transfer from cloud, respectively.

C. LATENCY BREAKDOWN WITH VS. WITHOUT OPTIMIZATIONS

For the third set of results we analyzed the overall application resumption latency for the UE with and without our proposed token reuse and data prefetching optimizations. The key stages involved in the MEC application resumption are listed in Table 5. The UE attached to the MEC in the U1 stage, became authenticated in the U2 stage, and application was resumed for the UE in the U3 stage. The U2 stage required the MEC in the foreign network to fetch the subscription data from the UE's home network (M1). Similarly, the U3 stage required the MEC to fetch the state data from the UE's home network (M2). The M3 stage was not involved in the MEC application resumption time and was needed for the UE to move to another MEC later. Fig. 8 shows the time taken by each stage for the two scenarios; without and with our proposed token reuse and data prefetching optimizations.

TABLE 5. Stages in MEC application resumption.

Name	Stage involving UE	Name	Stage involving MEC
U1	UE Attach	M1	Fetching Subscription Data
U2	UE Auth	M2	Fetching State Data
U3	Application Resumption	M3	Notifying Neighbour MECs

In both the scenarios, the authentication server was located in the MEC and the state size was 1 MB. Without optimizations, the M1 stage took place during the U2 stage while the M2 and the M3 took place during the U3 stage. As Fig. 8 shows, the M1 and the M2 stages induced an additional latency of 321 ms and 297 ms, for the two stages. We started the M1 and the M2 stages earlier, during the U1 stage, to reduce the time taken by the U2 and U3 stages, as seen in the lower half of Fig. 8. It can also be seen that the M1 and M2 stages were completed before they were needed by the U2 and the U3 stages. The reuse of the authentication token of the app server further reduced the latency of the U2 stage. The rest of the time taken by the U2 and U3 stages was mainly because the communication between UE and application server which could not be further reduced. We therefore suggest that mobile network operators deploy the proposed token reuse and data prefetching optimizations as these reduce the latency of the U2 and U3 stages by 56.3% and 28.3%, respectively.

D. SERVICE INTERRUPTION LATENCY

When the UE detached from one MEC and attached to the MEC in another MNO, the service was interrupted until the application for the UE was resumed. The service interruption latency was divided into four stages: UE attach, UE authentication, MEC to MEC communication for state transfer, and MEC to UE communication. We calculated this service interruption latency for three different scenarios, which are described in Table 6. The first considered the authentication server in cloud and transferred the state via the cloud without data prefetching and token reuse optimizations. The second considered the authentication server in MEC and transferred the state via the MEC proxy without data prefetching and token reuse optimizations. The third scenario considered the authentication server in MEC and transferred the state via the MEC proxy with data prefetching and token reuse optimizations (i.e. our proposed FS3A).

The comparison of service interruption latency for these 9, which shows that, with our proposed architecture and token reuse and data prefetching optimizations (scenario 3), service interruption latency was 2.96 seconds, that is 73.6% and 33.1% less compared to scenarios 1 and 2, as a result of the

TABLE 6. Scenarios for measuring service interruption time.

Scenario	Server Location	State Transfer via	Data Prefetching & Token Reuse
1	Cloud	Cloud	No
2	MEC	MEC Proxy	No
3	MEC	MEC Proxy	Yes

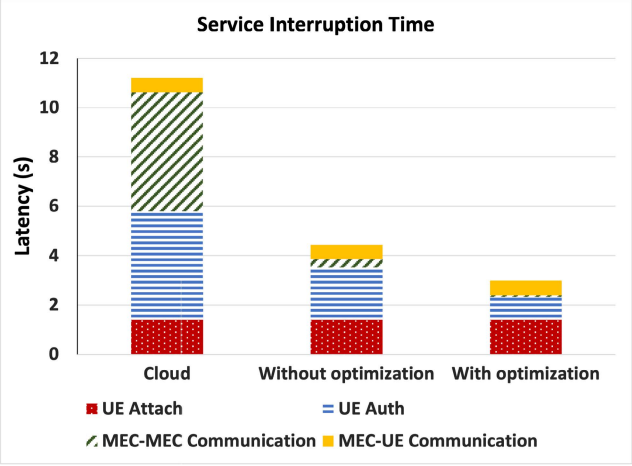


FIGURE 9. Service interruption latency comparison.

MEC proxy, token reuse, and data prefetching. It should be noted that the UE attach and the MEC to UE communication stages took almost the same amount of time in all three scenarios as they mostly depended upon propagation delay and could not be reduced. It can be seen that we reduced the UE authentication time, and MEC to MEC communication time by token reuse and data prefetching optimizations. If we ignore the time taken by the UE attach and the MEC to UE communication stages, the latency for scenario 3 can be further be reduced by 59.7% compared to scenario 2, which is a considerable decrease in service interruption latency.

VII. CONCLUSION AND FUTURE WORK

MEC is one of the most important technologies in 4G/5G networks as it brings computational services closer to end users. MECs are deployed by various mobile network operators and, in future, mobile users will have to face authentication and application mobility issues when they move from one MNO to another MNO. It would be a tedious task to buy subscriptions from multiple MNOs in order to benefit from a continuous MEC experience. In order to address these issues, we propose the FS3A mechanism for third-party authentication and low-latency state transfers between MECs and across different MNOs. FS3A makes use of a transparent proxy to provide seamless and fast 3rd-party authentication and application mobility while achieving low latency via authentication token reuse and subscription, and state data prefetching. The results show that:

- ***Reusing authentication tokens reduces authentication latency.*** FS3A saves 2543 ms and 701 ms on average by reusing the tokens from authentication servers in cloud and MEC respectively.
- ***Subscription data prefetching reduces the access control latency.*** FS3A reduces the access control latency by 88.6% by prefetching the subscription data.
- ***State data prefetching becomes crucial as the state size increases.*** State transfer latency is reduced by 51.4–91.3% for state of size of 10KB–10MB via state prefetching.
- ***Token reuse and prefetching play an important role in latency reduction.*** Token reuse and prefetching optimizations resume the application by taking 33% less time compared to no token reuse and prefetching.

This work addressed the authentication and application handover problem between the MECs that belong to multiple cellular service providers and propose a horizontal federation among MECs. In future, we will extend this work to form a federation among different service providers such as cloud, edge, and fog in order to create vertical and hybrid federations. This work can also be extended in another direction by considering other federation issues, apart from authentication and application mobility, such as traffic offloading, load balancing and capacity sharing between multiple MNOs.

REFERENCES

[1] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, pp. 637–646, May 2016.
[2] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1160–1192, 2nd Quart., 2021.
[3] Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, "Toward edge intelligence: Multiaccess edge computing for 5G and Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6722–6747, Aug. 2020.
[4] *Multi-Access Edge Computing (MEC) MEC 5G Integration*, document GR MEC 031 V2.1.1, ETSI, 2020.
[5] *Multi-Access Edge Computing (MEC): Phase 2: Use Cases and Requirements*, document GS MEC 002 V2.1.1, ETSI, 2018.
[6] U. Ahmed, I. Raza, O. Rana, and S. A. Hussain, "Aggregated capability assessment (AgCA) for CAIQ enabled cross-cloud federation," *IEEE Trans. Services Comput.*, early access, Jun. 16, 2021, doi: 10.1109/TSC.2021.3073783.
[7] *Multi-Access Edge Computing (MEC): Terminology*, document GS MEC 001 V2.1.1, ETSI, 2019.
[8] *Mobile Edge Computing (MEC): End to End Mobility Aspects*, document GR MEC 018 V1.1.1, ETSI, 2017.
[9] *Multi-Access Edge Computing (MEC): Application Mobility Service API*, document GS MEC 021 V2.1.1, ETSI, 2020.
[10] C.-Y. Li, Y.-D. Lin, Y.-C. Lai, H.-T. Chien, Y.-S. Huang, P.-H. Huang, and H.-Y. Liu, "Transparent AAA security design for low-latency MEC-integrated cellular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3231–3243, Mar. 2020.
[11] A. Ali, Y.-D. Lin, C.-Y. Li, and Y.-C. Lai, "Transparent 3rd-party authentication with application mobility for 5G mobile edge computing," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2020, pp. 219–224.
[12] F. Giust, G. Verin, K. Antevski, J. Chou, and Y. Fang, "MEC deployments in 4G and evolution towards 5G," *ETSI White Paper*, vol. 24, pp. 1–24, Feb. 2018.
[13] *Multi-Access Edge Computing (MEC) Framework and Reference Architecture*, document GS MEC 3, ETSI, 2019.

[14] A. C. Donald and L. Arockiam, "A secure authentication scheme for mobicloud," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2015, pp. 1–6.

[15] E. Bonnah and J. Shiguang, "Decchain: A decentralized security approach in edge computing based on blockchain," *Future Gener. Comput. Syst.*, vol. 113, pp. 363–379, Sep. 2020.

[16] Y. Targali, V. Choyi, and Y. Shah, "Seamless authentication and mobility across heterogeneous networks using federated identity systems," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2013, pp. 1232–1237.

[17] V. K. Choyi and A. Brusilovsky, "Seamless authentication across multiple entities," U.S. Patent 14 779 584, Feb. 18, 2016.

[18] E. K. Kiyemba Edris, M. Aiash, and J. K.-K. Loo, "Network service federated identity (NS- FId) protocol for service authorization in 5G network," in *Proc. 5th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Apr. 2020, pp. 128–135.

[19] Q. Cui, Z. Zhu, W. Ni, X. Tao, and P. Zhang, "Edge-intelligence-empowered, unified authentication and trust evaluation for heterogeneous beyond 5G systems," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 78–85, Apr. 2021.

[20] K. Han, M. Ma, X. Li, Z. Feng, and J. Hao, "An efficient handover authentication mechanism for 5G wireless network," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–8.

[21] W. Niewolski, T. W. Nowak, M. Sepczuk, and Z. Kotulski, "Token-based authentication framework for 5G MEC mobile networks," *Electron. J.*, vol. 10, no. 14, pp. 1724–1744, Jul. 2021.

[22] S. D. A. Shah, M. A. Gregory, S. Li, and R. D. R. Fontes, "SDN enhanced multi-access edge computing (MEC) for E2E mobility and QoS management," *IEEE Access*, vol. 8, pp. 77459–77469, 2020.

[23] J. Mwangama, N. Ventura, A. Willner, Y. Al-Hazmi, G. Carella, and T. Magedanz, "Towards mobile federated network operators," in *Proc. 1st IEEE Conf. Netw. Softw. (NetSoft)*, Apr. 2015, pp. 1–6.

[24] E. Pencheva, D. Kireva, I. Atanasov, and V. Trifonov, "Open access to intersystem handover control using multi-access edge computing," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Jun. 2018, pp. 1–7.

[25] T. Ouyang, Z. Zhou, and X. Chen, "Follow me at the edge: Mobility-aware dynamic service placement for mobile edge computing," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 10, pp. 2333–2345, Oct. 2018.

[26] S. Wang, R. Urgaonkar, M. Zafer, and T. He, "Dynamic service migration in mobile edge computing based on Markov decision process," *IEEE/ACM Trans. Netw.*, vol. 27, no. 13, pp. 1272–1288, May 2019.

[27] A. Machen, S. Wang, K. K. Leung, B. J. Ko, and T. Salonidis, "Live service migration in mobile edge clouds," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 140–147, Feb. 2018.

[28] A. Aghdai, Y. Xu, M. Huang, D. H. Dai, and H. J. Chao, "Enabling mobility in LTE-compatible mobile-edge computing with programmable switches," 2019, *arXiv:1905.05258*.

[29] J. Lee, D. Kim, J. Park, and H. Park, "A multi-server authentication protocol achieving privacy protection and traceability for 5G mobile edge computing," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2021, pp. 1–4.

[30] Y.-D. Lin, D.-T. Truong, A. Ali, C.-Y. Li, Y.-C. Lai, and T.-M.-T. Dinh, "Proxy-based federated authentication: A transparent third-party solution for cloud-edge federation," *IEEE Netw.*, vol. 34, no. 6, pp. 220–227, Nov. 2020.

[31] A. Roos, M. Hartman, and S. Dutnall, "Critical issues for roaming in 3G," *IEEE Wireless Commun.*, vol. 10, no. 1, pp. 29–35, Feb. 2003.

[32] H. Inaba, K. Suzuki, and Z. Miao, "Implementing LTE international data roaming," *NTT DOCOMO Tech. J.*, vol. 15, no. 4, 2014. [Online]. Available: https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol15_4/vol15_4_004en.pdf

[33] B. Mafakheri, A. Heider-Aviet, R. Riggio, and L. Goratti, "Smart contracts in the 5G roaming architecture: The fusion of blockchain with 5G networks," *IEEE Commun. Mag.*, vol. 59, no. 3, pp. 77–83, Mar. 2021.

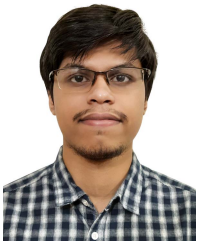
[34] *Openairinterface*. Accessed: Jun. 1, 2021. [Online]. Available: https://openairinterface.org/

[35] *Oai/Openairinterface5g*. Accessed: Jun. 1, 2021. [Online]. Available: https://gitlab.eurecom.fr/oai/openairinterface5g

[36] Osmocom. *Osmocom/Libgtpnl*. Accessed: Jun. 1, 2021. [Online]. Available: https://github.com/osmo- com/libgtpnl

[37] *P1sec/Pycrate*. Accessed: Jun. 1, 2021. [Online]. Available: https://github.com/P1sec/pycrate

ASAD ALI (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering from the University of Engineering and Technology, Taxila, in 2012, and the master's degree in electrical engineering from the National University of Science & Technology (NUST), Pakistan, in 2015. He is currently a Ph.D. Researcher with the Electrical Engineering and Computer Sciences Department, National Yang Ming Chiao Tung University (NYCU), Taiwan. His research interests include network security, network protocols, wireless communications, artificial intelligence wireless, network design, and optimization.



SAMIN RAHMAN KHAN is currently pursuing the B.S.Engg. degree in computer science and engineering with the Bangladesh University of Engineering and Technology (BUET), Bangladesh. He has stepped into research, through working on multi-access edge computing and mobile networking technologies. His research interests include computer networking, security, and applied machine learning.

SADMAN SAKIB is currently pursuing the B.S. degree in computer science and engineering with the Bangladesh University of Engineering and Technology (BUET), Bangladesh. His research interests include edge computing, the IoT security, computer networks, and applied machine learning.

MD. SHOHRAB HOSSAIN (Member, IEEE) received the Ph.D. degree in computer science from the University of Oklahoma, USA, in 2012. He is currently a Professor of computer science and engineering at the Bangladesh University of Engineering and Technology (BUET), Bangladesh. He has published more than 75 technical research papers in leading journals and conferences. His research interests include mobile malware detections, cyber security, software-defined networking (SDN), security of mobile and ad hoc networks, and the Internet of Things. He has been serving as a TPC Member for the IEEE GLOBECOM, IEEE ICC, IEEE VTC, *Wireless Personal Communication* (Springer), *Journal of Network and Computer Applications* (Elsevier), and IEEE Wireless Communications.

YING-DAR LIN (Fellow, IEEE) received the Ph.D. degree in computer science from the University of California at Los Angeles (UCLA), in 1993. Since 2002, he has been the Founder and the Director of the Network Benchmarking Laboratory. He is currently a Chair Professor of computer science at the National Yang Ming Chiao Tung University (NYCU), Taiwan. He published a textbook, *Computer Networks: An Open Source Approach*. His research interests include network security, wireless communications, and network softwarization. He has served or is serving on the editorial boards for several IEEE journals and magazines, and was the Editor-in-Chief of the IEEE Communications Surveys and Tutorials, during 2017–2020.