

End User Authentication Method in Mobile Edge Computing

By
Sadia Rahman Smita
ID: 151-19-1689
&
Md. Sabbir Hossain
ID: 151-19-1678

This Report Presented in Partial Fulfillment of the Requirements for the Degree of
Bachelor of Science in Electronics and Telecommunication Engineering
(B.Sc. in ETE)

Supervised By

Engr. Md. Zahirul Islam
Assistant Professor
Department of ICE
Daffodil International University

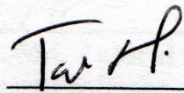


Department of Information and Communication Engineering
Daffodil International University
Dhaka, Bangladesh
January, 2019

APPROVAL

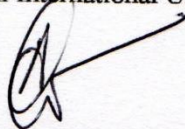
The Thesis titled “**End User Authentication Method in Mobile Edge Computing**” submitted by Sadia Rahman Smita ID: 151-19-1689 & Md. Sabbir Hossain ID: 151-19-1678 to the Department of Information and Communication Engineering, Daffodil International University, has been accepted as appeasement for the partial fulfillment of the requirement for the degree of Bachelor of Science in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation was held on January, 2019.

BOARD OF EXAMINERS



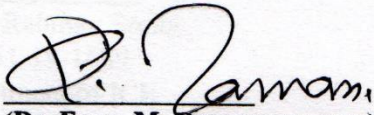
(Md. Taslim Arefin)
Associate Professor & Head
Department of ICE
Faculty of Engineering
Daffodil International University

Chairman



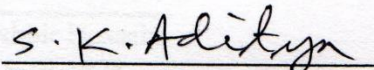
(Dr. A.K.M Fazlul Haque)
Associate Dean
Department of ICE
Faculty of Engineering
Daffodil International University

Internal Examiner



(Dr. Engr. M. Quamruzzaman)
Professor
Department of ICE
Faculty of Engineering
Daffodil International University

Internal Examiner



(Dr. Subrata Kumar Aditya)
Professor
Department of EEE
University of Dhaka

External Examiner

DECLARATION

I hereby declare that this thesis Report has been done by us under the supervision of **Engr. Md. Zahirul Islam, Assistant Professor, Department of ICE**, and Daffodil International University. I also declare that neither this report nor any part of it has been submitted elsewhere for award of any degree.

Supervised By



Engr. Md. Zahirul Islam
Assistant Professor
Department of ICE
Daffodil International University

Submitted By



Sadia Rahman Smita
ID: 151-19-1689
Department of ICE
Daffodil International University



Md. Sabbir Hossain
ID: 151-19-1678
Department of ICE
Daffodil International University

ACKNOWLEDGEMENT

Firstly, we would like to forward my regard to Almighty Allah for showing me the right path while attempting the duty.

The real spirit of achieving a destiny is through the path of eminence and solid discipline. we would have never achieved in finishing my job without the alliance, inspiration and assist issued to me by different personalities.

This thesis report would not have been manageable without the assist and direction of **Engr. Md. Zahirul Islam**, Assistant Professor, Department of Information and Communication Engineering, Daffodil International University, under whose supervision we chose this topic.

We would like to express my earnest respect to **Md. Taslim Arefin**, Associate Professor & Head, Prof. **Dr. A.K.M. Fazlul Haque** and Prof. **Dr. Engr. M. Quamruzzaman** Department of ICE, for their kind help to finish our project and also to other faculty member and the staff of ICE department of Daffodil International University.

We would like to thank our entire course mate at Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

Sadia Rahman Smita

&

Md. Sabbir Hossain

DEDICATION

**THIS THESIS IS DEDICATED
TO
OUR PARENTS
AND
OUR RESPECTED TEACHER**

ABSTRACT

Mobile Edge Computing (MEC) provides mobile and cloud computing capabilities within the access network, and aims to unite the telco and IT at the mobile network edge. The main feature of MEC is to push mobile computing, network control and storage to the network edges (e.g., base stations and access points) so as to enable computation-intensive and latency-critical applications at the resource-limited mobile devices. MEC promises dramatic reduction in latency and mobile energy consumption, tackling the key challenges for materializing 5G vision. A main thrust of MEC research is to seamlessly merge the two disciplines of wireless communications and mobile computing, resulting in a wide-range of new designs ranging from techniques for computation offloading to network architectures. In this report, a secured authentication method is proposed to enhance the security of MEC.

Table of Content

	Content	Page No.
	Declaration	ii
	Acknowledgment	iii
	Dedication	iv
	Abstract	v
Chapter 1: Introduction		1-4
1.1	General Introduction	1
1.2	Motivation	2
1.3	Related Work	3
1.4	Organizes of Thesis	4
Chapter 2: Mobile Edge Computing		5-17
2.1	Introduction	5
2.2	History of Mobile Edge Computing	5
2.3	Principle of Mobile Edge Computing	5
2.4	Working Technique of Mobile Edge Computing	6
2.5	Mobile edge Computing Standards	8
2.6	Mobile Edge Computing Mechanism	10
2.7	Mobile Edge Computing Characterize	10

Content	Page No.
2.8 Mobile Edge Computing Architecture	11
2.9 Design and Implementation	12
2.10 Using MEC in IOT Device	14
Chapter 3: Security Features in Mobile Edge Computing	18-22
3.1 Introduction	18
3.2 The Importance of Security in Edge Paradigms	18
3.3 Security Concern	19
Chapter 4: Proposal Authentication Method	23-26
4.1 Introduction	23
4.2 Proposed Authentication Method	23
Chapter 5: Result & Analysis	27-29
5.1 Experimental Setup	27
Chapter 6: Conclusion	30
Reference	31

List of Figures

Chapter 2

Fig 2.1	Technique of Mobile Edge Computing	6
Fig 2.2	Mobile Edge Computing Mechanism	10
Fig 2.3	Mobile Edge Computing Architecture	11
Fig 2.4	Components in MEC server	12
Fig 2.5	Components in eNode B	13
Fig 2.6	Traffic Workflow in MEC	14
Fig 2.7	Based Video Surveillance	15
Fig 2.8	MEC-Based Mobile IOT Scenario	16

Chapter 4

Fig 4.1	Connection End users to Cloud	24
Fig 4.2	User Connects to Cloud server through Authentication server	24
Fig 4.3	Authentication server include in MEC	26
Fig 4.4	Flow chart of AS in MEC	26

Chapter 5

Fig 5.1	Experimental setup of MEC	28
Fig 5.2	Comparative Energy Consumption Graph	28
Fig 5.3	Packet Overhead Consumption Graph	29

Chapter 1

Introduction

1.1 General Introduction

Mobile Edge Computing (MEC) is another innovation, now which is being the standard ETSI Industry Specification Group (ISG) technology. The Mobile Edge Computing technology offers an IT service and cloud computing capability close to mobile network radio stations (RAN) and close to mobile subscribers. The goal is to minimize latency, provide high-efficiency networking and service, and provide improved user experience. The ambition of MEC is to reduce latency, establish highly efficient network operation and service delivery, and offer an upgraded user experience. Mobile Edge Computing is uniformly developed by the progression of mobile base stations and the merging of IT and telecommunications networking. Stand on a virtualized platform, MEC is perceived by the European 5G PPP (5G Infrastructure Public Private Partnership) explore body as one of the key developing technologies for 5G networks (additionally Network Functions Virtualization (NFV) and Software-Defined Networking (SDN)) [1]. Along with characterizing further developed air interface technologies, 5G networks will use increasingly programmable entrances to deal with software network and use IT virtualization technology widely through the telecommunications infrastructure, capacities, and applications. For permitting the progression to 5G by MEC expressed as a key technology and architectural concept, after all it helps advance the change of the mobile broadband network into a programmable world and devote to fulfilling the requirement of 5G as far as expected all through latency, scalability and automation. MEC is depends on a virtual stage, with an approach correlative to NFV: literally while NFV is centered on system, the MEC framework empowers applications running at the edge of the network. The foundation of MEC and NFV or network function is very comparable. As follows that one operator may get benefits as much as possible from their investment. It will be so favorable for reusing the infrastructure and infrastructure the executives of NFV to the biggest extent possible by facilitating both VNFs (Virtual Network Functions) and MEC applications on the similar platform. Mobile Edge Computing can be characterized by low latency, proximity, high bandwidth, and real-time insight through to radio network information and location awareness. All of this can be converted into amount and can make

on the off chances for mobile operator applications and substance providers empowering hem to play integrally and profitable aspects not over their own business models and the mobile broadband allowed them for sensing better monetized. For giving the services to clients and certain clients along with adjoining industries through MEC that would now bear their mission-critical application over the mobile network. It permits a new value chain, fresh business opening and a bunch of new use cases over various sectors. The aim is to establish a good economic situation which will make feasible business for all players in the value chain and to encourage worldwide market development. The capable and coherent combination of such applications over multi-vendor Mobile Edge Computing platforms, a standardized in open environment need allow for creating. This will likewise ensure that by far most of the clients of a mobile operator can be provided. The goals of this research pepper to introducing Mobile Edge Computing, security features in MEC. Mainly how can MEC system we can create an authentication method for robust the security in MEC.

1.2 Motivation

Low latency and jitter, context awareness, mobility support etc. all this characteristic is missing in cloud computing paradigm. Absence of this property that is compelling for several applications (e.g. vehicular networks, augmented reality). Fog computing, mobile edge computing mobile cloud computing and so on this type of various paradigms can full-fill this requirements. These edge paradigms share several appearance. Cloud computing put forward some storage, information, data of users to MEC. In this case MEC is known as mini cloud. MEC stand on near the user client so that users can experience better performance from cloud through MEC. MEC can be provided all of the requirements which is missing in cloud (e.g. low latency, jitter, mobility support).

Mobile Edge Computing (MEC) is a developed architecture where cloud computing services are extended to the edge of networks leveraging mobile base stations. Mobile Edge Computing as a promising technology it is totally wireless technology. In MEC using software and hardware platforms, located in the vicinity of end users at the edge of the network in mobile edge computing mobility is needed because it is wireless technology. Sometimes it experienced eavesdrop. Man-in-middle attack, DOS (denial of service attack) etc. this type of attack can be held in MEC. This attack only held because of user un-

authorization. In this research pepper we are shown the authorization in MEC for increasing security in MEC.

1.3 Related work

Currently, there is no research that identifies and authenticates the members of a global infrastructure of interconnected data processing centers owned by different companies and individuals. However, you can look for a problem in other areas, such as federally cloudy calculations and equivalent peer-to-peer calculations then we can look up the real problems. Indeed, there are many ways to build an inter-agency compliance management system. [1] Such views use different standards, such as SAML and Open ID, to provide authentication of single sign-on (SSO) authentication. There are several mechanisms for peer-to-peer computing provides mutual authentication without connecting to the centralized authentication server. [2] Since these approaches are compatible with the basic infrastructure of boundary paradigm design, these approaches can be adapted to authenticate the extreme datacenters belonging to different domains of trust. On the other hand, there are genuine original backgrounds that integrate user authentication on the same trust domain, which are specific to paradigms. For example, Donald and others have identified a centralized infrastructure for MCC, which serves as one trusted third-party server authentication. However, this method requires an authentication server is always available, so their use is limited. Ibrahim, another worker [3] any fog has developed a user authentication system that allows a user to authenticate with each other, and this method forces all fog nodes to store certain credentials for all users of a trusted domain. There is another MACs and fog that have more credibility, even if the server authentication is no more there, even though the authentication server is not available. It can be reached by tying it coupling the cryptosystem & using hardware or of mixed breed encryption (public key and symmetric key encryption) .While these mechanisms focus on authenticating the user, they are the same domain of trust that the federation has. More precisely, since the end-user data center has extreme datacenters in the title of authentication, Empiric has access to information that provides different original systems use location-based. For example, in conjunction with federated mobile cloud reports, Shouhuai et al [4] Situation concept authenticity, on the basis of the concept of "brotherhood", "wherever you are", "where you are" & "what's this time". The other authors, such as Bouzefrane [5] Usages the NFC (Near Field Communication) function to verify that the mobile device is downloading

jobs to the native cloud. It Observer plats based authentication can be explored in a number of other areas (for example, wireless sensor networks, Internet surfing) and provides different mechanisms for adapting to the latest paradigms. When it comes to user mobility, MCC script has few protocols that attempt to make reliable & effective authentication. For example, Young et al [6] providing efficient design for that, allowing the users of mobile to move different region to region. Keep in mind that these protocols typically require access to the server authenticating in the centralized cloud infrastructure, much other issue to open for improvements. At the end, some border paradigms allow users to place their own personal data centers. Consequently, some works, such as the structure of OPENi [7] on how to access external users on these platforms in the cloud. The OPENi Authentication ingredient uses the Open ID connection authentication level between other mechanisms. Hence, the owner of the cloudlet decides that server's authentication and users who have access to the cloudlet resources will be allowed to trust.

1.4 Organization of the Thesis:

The first chapter contains motivation and goal of the thesis work.

Second chapter brief details of Overall view Mobile Edge Computing (MEC), including with MEC architecture and applications.

Chapter three contains of security threats and mechanism in MEC

Chapter four is brief details of overview end user authentication robust in MEC

Chapter five contains result and performance analysis

Last of **Chapter six** conclusion

Chapter 2

Mobile Edge Computing

2.1 Introduction

Mobile Edge Computing (MEC) is the term which refers to IT services offered to application developers content providers at the edge of the wireless telecom network. High bandwidth, low latency and time based access to radio network are offer in mobile edge computing. These MEC services are utilized by applications. [8]

2.2 History of Mobile Edge Computing

Edge mobile computing term is standardized by the European Telecommunications Standards Institute (ETSI) and Industry Specificity (ISG). According to ETSI, mobile edge calculation is defined as[9]

“Mobile Edge Computing provides an IT service environment and cloud computing capabilities at the edge of the mobile network, within the Radio Access Network (RAN) and in close proximity to mobile subscribers.”

2.3 Principle of Mobile Edge Computing

Principles of main mobile edge paradigms are:

- 1. Provide cloud capability through RAN:** Mobile Edge Computing (MEC) allows a distributed computing domain for application and service hosting through radio access network (RAN). Applications can be exposed to real-time RAN information. [10]
- 2. Avoid Bottlenecks & system Failure:** Whereas MEC provides distributed cloud computing capacity at the base station so it serves avoid bottlenecks and system failure.

3. **Ultra low latency:** Deploying MEC in close proximity with end user within the RAN it's allow direct to this traffic between home network and end client. Therefore the users of MEC can they get the service of ultra-low latency.

4. **Support Mobility:** Mobility support is the major requirement of many systems in the long run, as missed or overlapping data can cause severe consequences. To support mobility, the IoT system must be equipped with a transmission or transmission mechanism that is responsible for registering the sensor node from the initial access point and registering it to the new access point. Due to the stringent security requirements, delays, network coverage and reliability, it is difficult to introduce an advanced transmission mechanism to support full mobility in complex domains such as health. This issue is far more complicated for Mobile edge-assisted IoT systems as smart gateways at the edge provide dedicated storage and edge services. Service Module needs effective service for updating and synchronizing the distribution repository when dealing with mobility.[20]

2.4 Working Technique of Mobile Edge Computing:

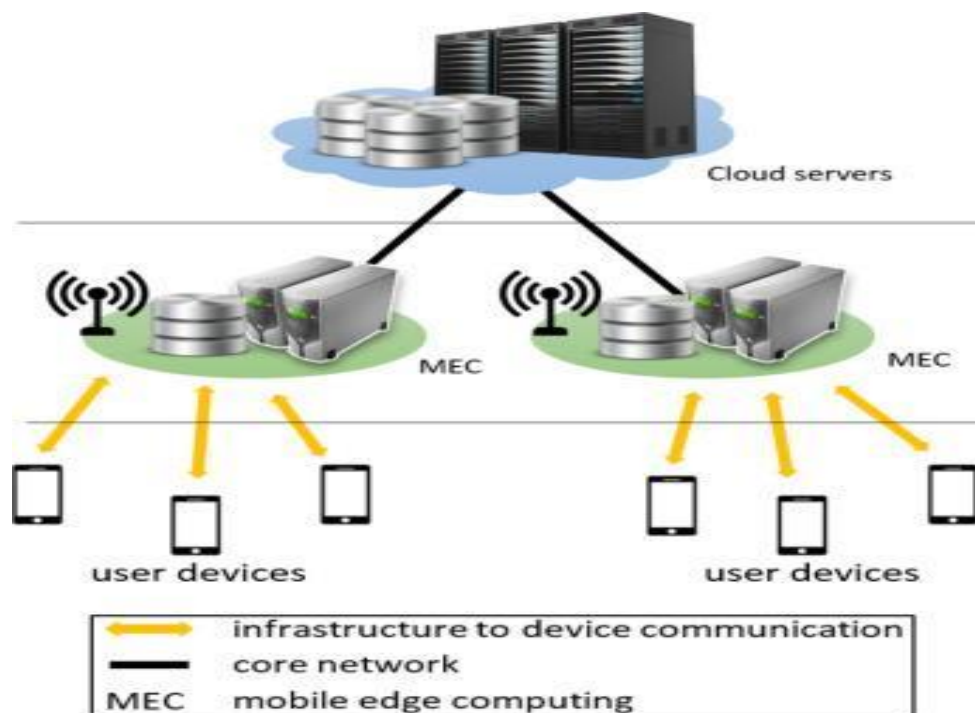


Figure 2.1: Technique of Mobile Edge Computing

A. Mobile Edge Computing in Outdoor Scenario:

There are distinctive approaches to actualize Mobile-edge Computing, contingent upon the entrance innovation. For outside, Macro cells sellers insert anchored processing and virtualization abilities straightforwardly into radio access organize components. This mix of uses with radio gear enables administrators to quickly convey inventive system highlights, quicken over-the-top (OTT) benefits and empower an assortment of new high esteem administrations. Such adaptable administrations are executed at an extremely key area in the versatile system, making them substantially more fundamental than some other applications keep running at the center. This design is especially applicable to: [11]

- Improve portable clients' Quality of Experience (QoE), by lessening inactivity, enhancing nature of administration or/and giving modified administrations.
- Improve framework's proficiency, with increasingly insightful and upgraded systems.
- Enable troublesome vertical administrations, especially pertinent for Machine-to-Machine situations, Big Data the executives, Analytics, Smart Cities and substantially more.
- Tight combination with radio hardware, making it straightforward traffic qualities and necessities, manage radio conditions, get gadget area data, and so on.

B. Mobile Edge computing in indoor Scenarios:

With regards to indoor, for example, Wi-Fi and 3G/4G passageways, edge mists appear as incredible on-premises entryways, where committed insight fills neighborhood needs. Through lightweight virtualization, those portals run various administrations connected to the specific area they are introduced in, for example,

- Machine-to-Machine situations: Connecting to different sensors, Mobile-edge Computing administrations can manage a wide range of checking exercises (cooling, lifts, temperature, moistness, get to control, and so forth.)
- Retail Solutions: Having the capacity to find and speak with cell phones, there is a chance to convey higher incentive to the shoppers and the shopping centers. For instance

conveying content dependent on area, executing increasing reality, enhancing the general shopping background, or managing an chord online installment.

- **Stadiums, Airports, Stations, Theaters:** Specific administrations can help oversee different sorts of crowded places, specifically to manage wellbeing, security, departure, or to give new sorts of administrations to the general population. For instance, arenas could give live substance to the general population; airplane terminals could manage travelers to their door through an increased reality benefit, and some more. Every one of these applications would use neighborhood substance and conditions to be consummately adjusted to their crowd.
- **Big information and Analytics:** Last yet not minimum, the data accumulated at this key point in the system, can be utilized as a major aspect of a greater investigation activity to serve clients better.

2.5 Mobile Edge Computing Standards

MEC Standards by the MEC ISG

- **End to End Mobility Aspects** — This standard addresses the problem of administrative progression when the client gadget is used when the external system is used and then leaves the system. It discusses procedures, solutions, and judgments for copying different scenarios to ensure consistent communication between the device and the network. [12]
- **Mobile Edge Management, Part 1:**
- **System, host, and platform management** — This standard describes the portable peripherals, hosts, and administrative conventions.
- **Bandwidth Management API** — This standard basically controls bandwidth issues when many devices use the same line. Software Policy Information and How to Apply Specific Application program Interface (API) Scenarios that Affect Broadband & Linear Borders.
- **UE application interface** — This standard can help you troubleshoot the program's lifecycle in the application interface of the device you are connecting to.

- **General Principles for Mobile Edge Service APIs** — This respected API consists of the glossary of the structural standards of the mobile service. This archive also shows APIs and templates.
- **Mobile Edge Management, Part 2** — MEC ISG draws a lifestyle management protocol for use in this standard. The document lists rules and management requirements. It also charted the reference points that support life cycle management.
- **Mobile Edge Platform Application Enablement** — This document focuses on how to extend applications to one (Mp1) mobile platform functionality to communicate with the mobile periphery.
- **Radio Network Information API** — Radio network information can be used with mobile extreme platforms to improve mobility. This standard shows how to order the Radio Line Information API and how to use it.
- **Location API:** This standard specifies the rules for determining the user's location information on the edge line.
- **Market Acceleration; MEC Metrics Best Practice and Guidelines** — This document lists the MEC criteria for MEC technology enhancements.
- **Technical Requirements** — These features are not related to the MEC, for example, non-specific NFV organization and mobility standards. It also explains the structure, service requirements, and lists the important features.
- **Framework and Reference Architecture** — This definition defines the MEC system and reference architecture. This is especially valuable because it refers to references in subsequent standard documents.
- **Terminology** — Glossary of terms related to different components of the MEC.
- **Service Scenarios** — Chart of services generated by MEC.
- **Proof of Concept (PoC) Framework** — it looks for the system PoC and its goals.

2.6 Mobile Edge Computing Mechanism

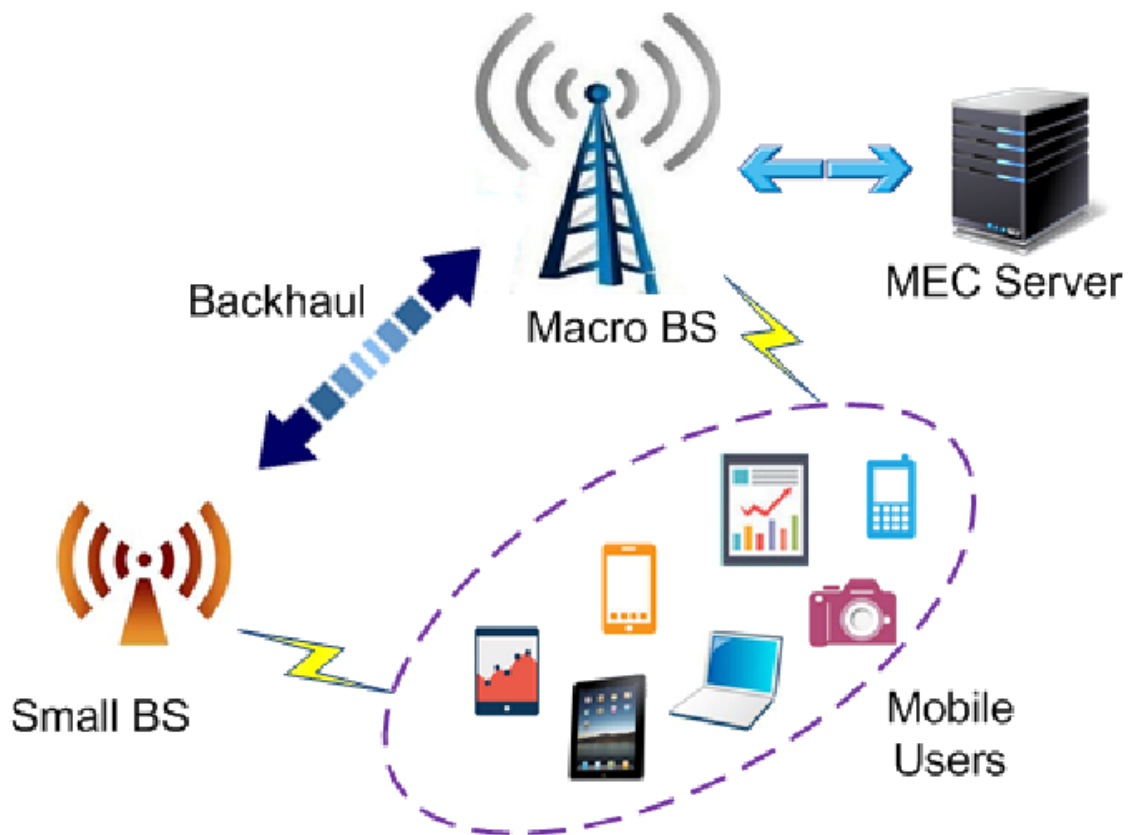


Figure 2.2: Mobile Edge Computing Mechanism

2.7 Mobile Edge Computing Characterize

As described on white paper published by ETSI, mobile edge calculations can be described as follows:

- 1) On-Premises: MEC platforms can be isolated from the rest of the network, while they are accessing local assets. This machine is very important for machine scripts. MEC isolated from different networks reduces vulnerability.
- 2) Proximity: Located closest to you, mobile edge computing has favorable position to investigate and materialize big data. It is additionally beneficial for compute-hungry devices, for example augmented reality, video analytics etc.

- 3) Lower latency: Edge paradigm services are sent at the closet area to user devices, isolating network information development from the central network. Consequently, user experience is accounted high quality with ultra-low latency and high bandwidth.
- 4) Location awareness: Mobile edge-Distributed devices use low-level signal to share data. MEC delivers data from nearby devices to the network and identifies where devices are located.
- 5) Network context information: Programs that provide networked information and real-time network data services benefit organizations and occasions by executing MEC in their plan of action. Based on RAN real-time information, these applications can access the congestion of the radio cell and network bandwidth. This will help them in future to make smart decisions for better conveyance of administrations to client delivery of services to customers.

2.8 MEC Architectures

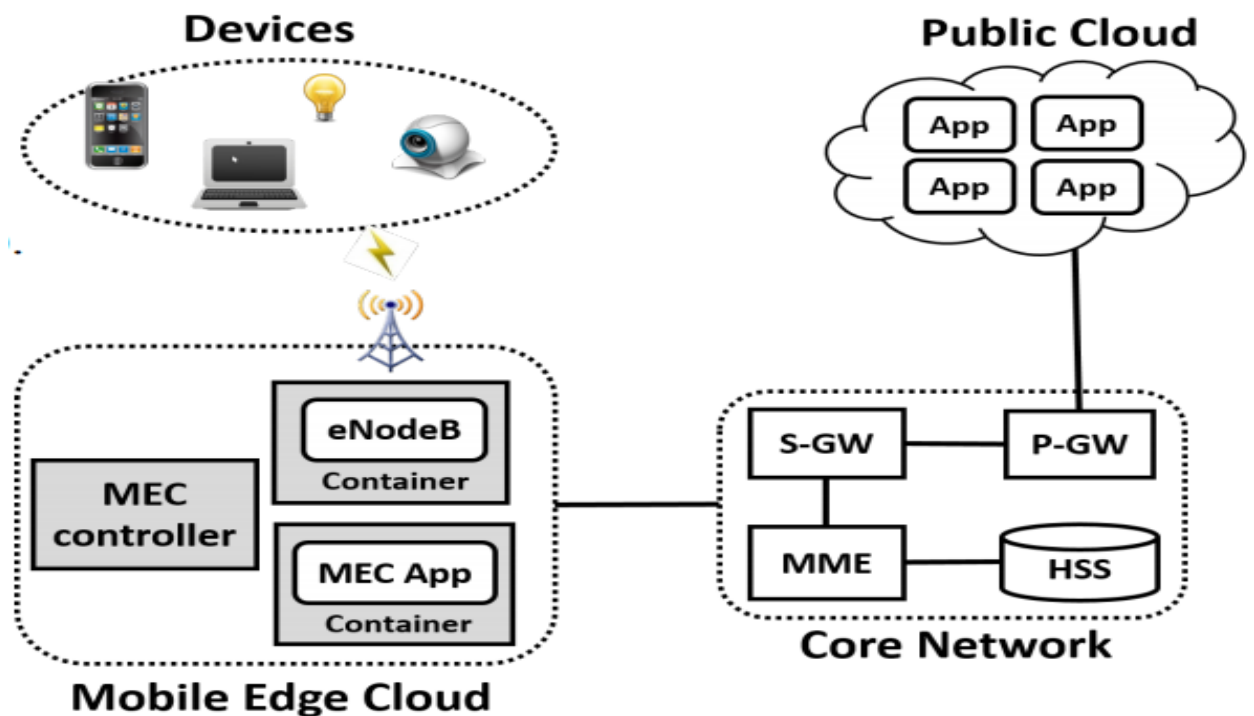


Figure 2.3: Mobile Edge Computing Architecture

- UE:
 - LTE dongle
- Mobile Edge Cloud:
 - Container-based e Node B (openairinterface5g).
 - MEC controller
 - MEC application (Docker image)
- EPC (open air-cn):
 - MME + HSS
 - S/P-GW
- Cloud:
 - Open Stack, Amazon EC2 [13]

2.9 Design and Implementation

The components of MEC

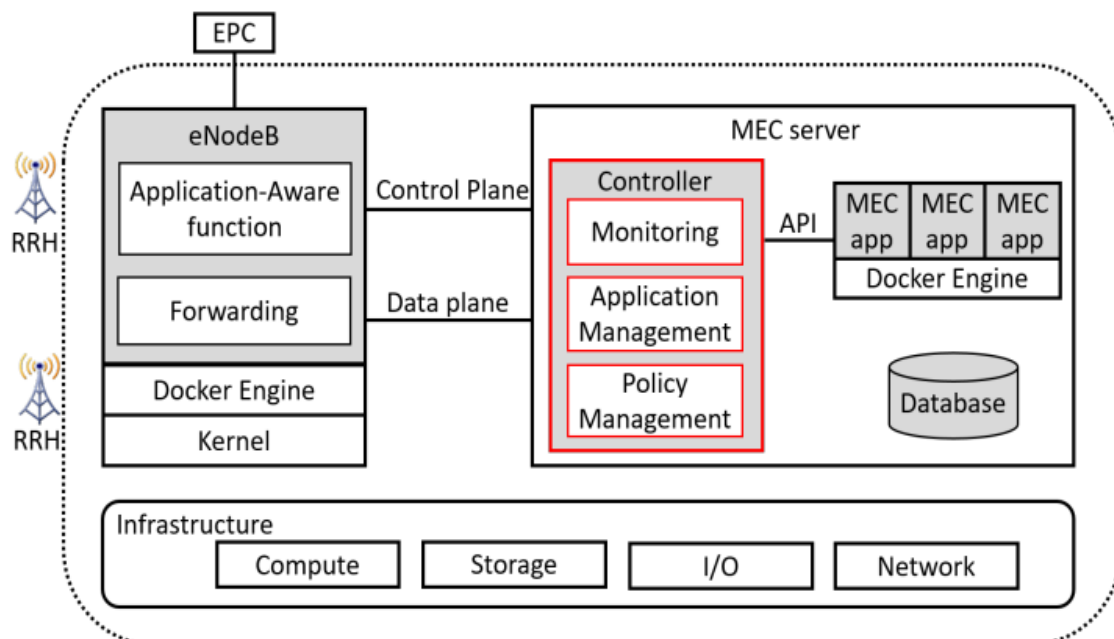


Figure 2.4: Components in MEC server

MEC controller:

- Monitoring
 - Monitor the throughput of each application.
- Policy Management
 - Maintain the application list.
 - Trigger redirection procedure.
- Application Management
 - Launch MEC application.
 - Release resource when application at idle for a long time.

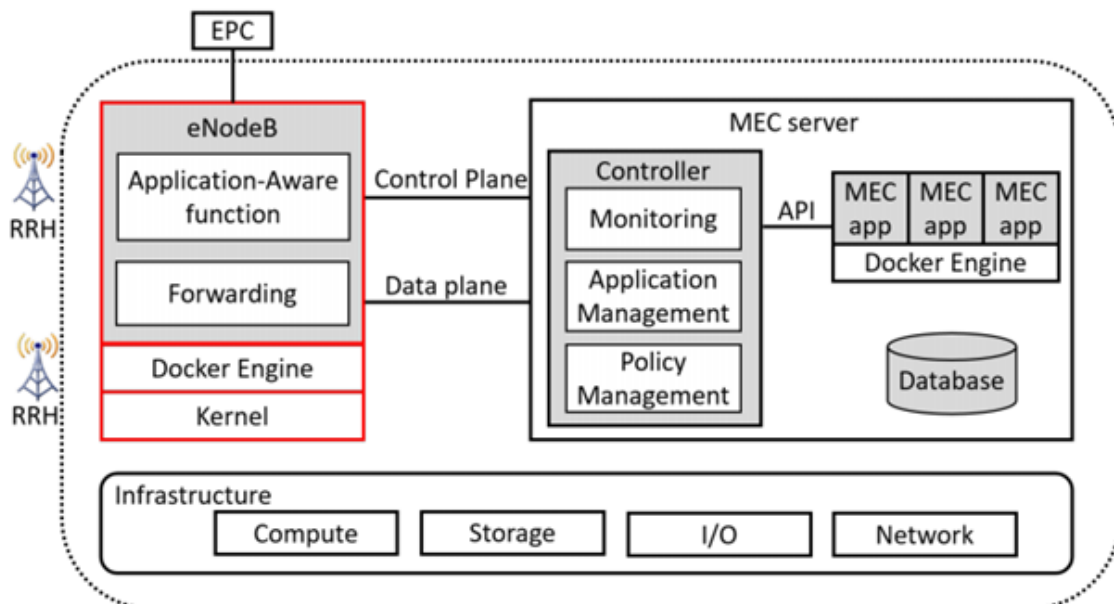


Figure 2.5: Components in eNode B

- Infrastructure:
 - General-purpose computer
- eNode B:
 - Low-latency kernel
 - Containerization
 - Application-aware function
 - Inspect packet header against the policy
 - Forwarding component
 - Send packets to MEC server

Traffic Redirection Workflow

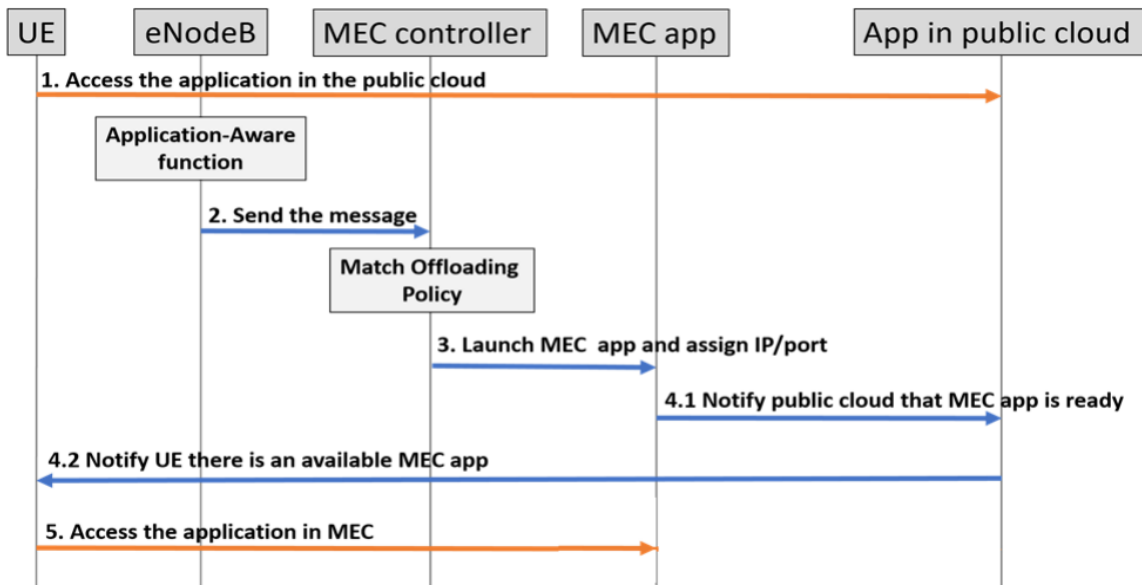


Figure 2.6: Traffic Workflow in MEC

2.10 Using MEC in IOT device

A. MEC in a IoT deployment for surveillance and safety

The exchange between the MEC and IoT concepts identifies situations where intensive computational load is required, such as video surveillance and cases where the object requires recognition. Open computing algorithms for image processing may be less communication delay to satisfy the overall delay budget included in the MEC host resource account and real-time automated tracking. This is done in the appendix and the S1-U condition is depicted in MEC on the basis of video surveillance alternative. A local network of IoT touch gadgets, for example, camcorders, is connected to a broadband cell network (for example, LTE network) with the nearby IoT gateway. [14]

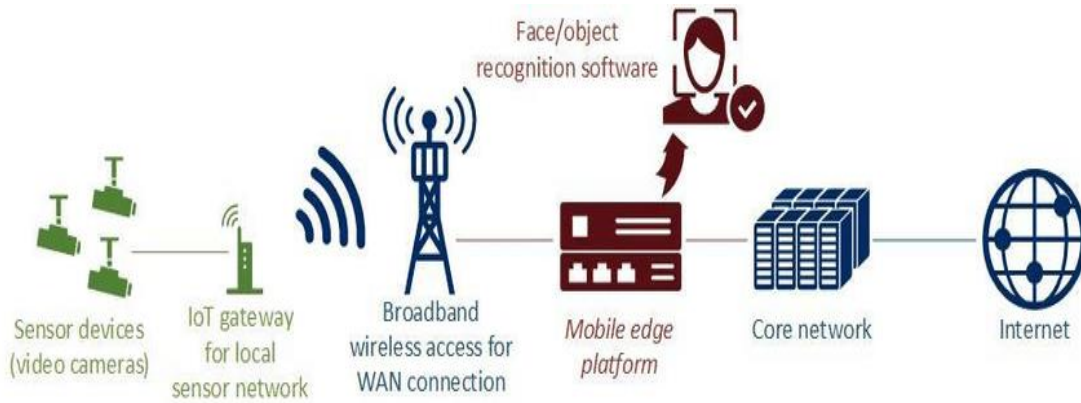


Figure 2.7: MEC- Based Video Surveillance

Video streams will be sent to the working ME host for the video watchdog application IoT. Real-time video editing is done so that the IoT control program sends a trigger to the central station where the video is recorded. This agreement does not allow mobile operator to send expensive equipment and accessibility functions using radio communication network and ME system.

B. MEC for IoT devices' capabilities offload

Thus, the various scenarios described above basically include static nodes, where mobility support is an important necessity. Several models can be installed in certain locations, even with water and electricity monitoring, home and industrial automation sensors, as well as wireless communication. Given the capabilities of such devices, the data handler and controller are hosted on the MEC host and are managed as Mobile edge applications. Using the rich features offered by the Mobile edge management, these applications can be instantly upgraded, shifted, and upgraded when you need it. From the perspective of deployment, the ME platform, which deploys IoT applications described in this and the previous paragraph, is a RAN (e.g. eNB, RNC) or RAN user interface (for example, S1-U). In this deployment option, the ME platform must be able to transfer data traffic from standard RAN user peripherals to Mobile edge applications without affecting the rest of the mobile network elements. For example, on an EPS-based mobile network, the above deployment version refers to redirecting GTP-encapsulated packets to the required MEC applications through the S1-U interface.

C. MEC for connected vehicles and moving IoT devices

Other important IoT usage conditions require that devices connect to a broadband cellular network, as well as be able to move across different cells that support mobility and session continuity. This may be the basis of IOT using airplanes, street cars and trains. Under these circumstances, the MEC version reveals some additional difficulties due to previous compatibility with older mobile networks. Indeed, mobility and session management are usually done by linear network functions such as Mobility Management Entity (MME), Serving Gateway (SGW), and Serving GPRS Support (SGSN) on the current 3G / 4G networks. Moving mobility support for the MEC phase may have a significant impact on the existing architecture as the inheritance parts should include non-standard mechanisms for linking the MEC platform, which should provide appropriate control plane information. At present the industry is very enthusiastic about promoting network gateways and basic functions. Virtualized EPC solutions provide easy and customized tracks to central network functions.

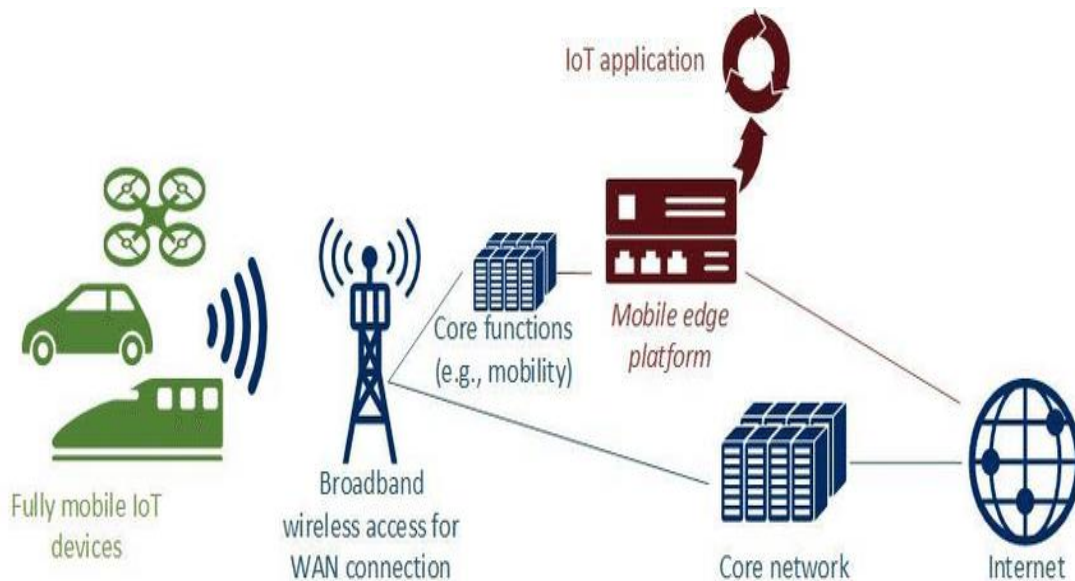


Figure 2.8: MEC-Based Mobile IOT Scenario

Approached from the line edge to help the MEC based IOT structure. In this educational option, MEC is placed in the client plane interface, which connects the mobile network to the rest of the packet data network, for example: SGi interface in EPS architecture (see

Figure 5). For IOT, ME applications do not require complex traffic filtering and monitoring to get the traffic required, and the MEC platform can be used to manage mobility, for example mobility, as well as other life prospects, QoS performance, charging, and more.

Chapter 3

Security Features in Mobile Edge Computing

3.1 Introduction

There are few difficulties that must be defeated so as to incubate community for biological where all players (specialist organizations, foundation suppliers, end clients) convenience than the administration given by illustrations edge. Naturally, mainly very principle of safety challenges. In this division, we will audit why safety is an extremely essential multiplier in this exceptional behalf and explore the specie threats that can target edge paradigms presents the prerequisites and Challenges of the security mechanisms that should be connect to this specific context. [16] There is an extensive request for secure and secured portable control. MEC offers new types of services, but it is rare peculiarities create new security and security issues. Most importantly, natural diversity of the MEC systems is that simple beliefs and original mechanisms cannot be used. Second, the diverse range technologies of the communication as the support of MEC and the programmatic nature of network administration mechanisms create new generation secure threats. In addition, the safe and personal computing system is very pleasant because extreme servers can be listener or attacker. [15]

3.2 The Importance of Security in Edge Paradigms

As it was said before, one of the biggest challenges for the production of peripheral paradigmatic ecosystems is security. And then there is no. of explanation.

First and foremost, the most extreme paradigm center has several powerful innovations for wireless networks, distributed and equal-level systems, and virtualization platforms. It is important not only for building blocks, but also for the organization of various security products. This, in turn, is a complex issue because we need to create an inextricable and horizontally perspective of all security systems that allow them to integrate and interoperate. [16]

Secondly, it is much more striking than the sum of all its components: we do not guarantee the safety of the entire system by ensuring the safety of all powerful innovations. Once cloud computing capabilities are transmitted to the edge of a network, new situations arise

(for example, collaboration between uneven data centers, migration services locally and globally), and their security is not envisaged. In addition, we must pay particular attention to the specific requirements of this specific context. It can use security mechanisms that can be used. For example, security mechanisms should be more independent and do not depend on the continuity of the centralized infrastructure. This section has two main objectives: not only the absence of a centralized management system (e.g. malicious attacks, interrupted communication, and distributed applications), but also the mechanisms that need to be taken into consideration in the security system delays.

Third, in addition to the security threats associated with certain peripheral features, the entire system also has security risks inherent in their construction blocks and application scripts. And this is not a trivial issue, because these threats are really important. The obvious example of this is the main mechanism of fogging calculations and the Internet of substances that are important in any of the extreme paradigms. In addition, we consider it to be a "blend of all of the above for all aspects of security": it is essential to ensure that multiple groups of technologies (from mobile to cloud), as well as global communications and access to heterogeneous ecosystems. This situation creates a considerable amount of attack, which also applies to all paradigms that use IOT.

In the end, it is very important for us to influence our society more effectively. The number of conditions that can be used to add end-to-end patterns is extremely high. Any aspect of our everyday life is affected by applications that are used in these infrastructure our personal information (e.g. photographs, medical reports), our daily work (e.g. transport, commerce), our business ecosystems (e.g. industries), our important infrastructure (for example, energy, emergency systems) and so on. Without security and privacy mechanisms, the benefits of peripheral paradigms quickly emerge from malicious opponents. [16]

3.3 Security Concerns

Edge paradigms components are CIA triad components, confidentiality, integrity, and availability are a sophisticated design for information security. To many various parts of faith that require the foundation of MEC.

Confidentiality: There is several programs presented edge of a network that serves mobile users, such as location information. Although these applications are useful, they also create

hidden threats. For example, No available rule defined for the user ID in the application layer separately from its geo-layout. Therefore, you need to enter new protocols to be prebled. Client data is vulnerable between mobile edge computing and cloud communications channels. Uses a location based attack, such as packet compression, location-based closing devices.

Integrity: Biological climate in mobile edge paradigm includes many artists, such as end-users, service providers, and infrastructure suppliers. This can cause a few security issues. Cloud servers allow them to efficiently compute sites to authenticate to administrative servers in datacenters, depending on their isolated environments, but are inaccessible to the open environment. For example, it would be difficult to share the MEC clusters with cloud servers under a managed domain. This scenario can cause several attacks, such as attacks on the attacker's central cloud systems, which can be ultimately authenticated and later stolen from their confidential information.

Availability: Depending on the isolated environment, the MEC system may be subject to Service of Denial (DOS) -based attacks. In a single hub, these attacks are not dangerous, but if there are correlation attacks on multiple geo-sites simultaneously, this can result in real consequences. For example, damaged sensors in the industrial sector are affecting globally. It is difficult to mitigate such attacks as the MEC system is directly connected to the latest devices and cannot detect malicious attacks on the network [17]

1. Network Security: Network Security, for example, cellular networks, or wireless networks, as well as various communication networks as a priority in the MEC is a very important element. Traditional network environment, network administrator, network traffic security barrier defines the network security policy. However, MEC may be located on the Internet can lead to interfere with the MEC and the network will be vulnerable to attacks, such as DOS, defines the management of sector all policies. Such attacks are limited to the MEC meeting and the communication network can be far more effective. Attackers can implement traffic or listening attacks that can enter the network or quantum network. Programmers commandeering the system stream can dispatch assaults to influence MEC framework execution. Man-in-the-center assault is probably going to be powerful while blocking information communication. Aggressors can effectively control the information making a trip from the cloud to the client and the other way around. It is difficult to mitigate such attacks, as virtual machines cannot be placed and blacklisted. Han

et al. Provided a measuring method for preventing user from connecting to the rouge gateways by tracking the rotating time between the user and the DNS server [17]

2) Core Network Security: it is necessary to mention the main network of all paradigms can be supported and most basic network security is activated via mobile nucleus networks or central cloud. Cloud services are often controlled by third-party vendors, such as Amazon, Microsoft, and Google. However, it is absurd to have full dependence on their security systems. Moreover, there is a high hazard for client's close to home and delicate data which can be stolen by malevolent substances. Edge gadgets trade data with one another and may sidestep the focal framework's security instrument. This makes security vulnerable and hack able. This sort of security issue won't influence the entire environment and will be constrained because of its decentralized nature. This destroys security vulnerabilities and security. Security concern of this type does not affect the entire environment and is limited due to decentralized nature. It also has the ability to change the system data and provide false information if the services can be stolen. This amount of impact is limited, but it can rule out the administrations. When the core of the center is in danger, it can break down several components of the central structure. The components of the implanted central system may break the structure of the lower level. Attackers have full access to information and may corrupt network data streams. [17]

3) MEC Server Security: Center system components that are imperiled can disturb the lower level framework. Center system components that are imperiled can disturb the lower level framework. Security channels may cause damage to the physical resources in the attack. This attack cannot be limited on the one hand, and a very important. Additionally, the data center's local scope and information flow can be abducted by users and malicious actors such as ASP. In addition, designer errors, configuration errors, security failures, or exploitative risks may be risky for data centers security. Recently introduced in the world of technology, MEC has some security expertise to ensure system security. If the access to the system is transferred to the resources of the MEC system, the attacker can either use the integrity of the system or can deny service attacks, attacks in the environment, and so on. Such services will be discontinued or interrupted as a result. Another problem with security is through the entire server farm. In this attack, all server farms are controlled by the uniqueness or interference of various attacks. Attacks can be a benefit or background.

Strong datacenters have a great impact on geographical locations, which can have a great impact. [17]

4) Virtualization Security: In the main cellular data center, multiple network instances are shared on a shared network. If one resource is malfunctioning, it can affect the virtualized infrastructure. The attacker can abuse and exploit the underlying asset. Service of Denial DOS attacks are good on the way. MEC virtualization frameworks can completely eliminate assets that account for computing, accumulation and system solutions. Users who connect to MEC virtual servers may opt out of requests or services. At the same time, rigid competitors can break virtual assets and depend on its framework and IOT gadgets. For example, any IOT device is located within the range of the radio network and may be malfunctioning and can be sabotaged. One of the safest situations is security spill. MEC is responsible for providing information about a few APIs that are implemented in the environment. Perhaps, these APIs are good on less well-off than any abusive one. Multiple attacks can be enhanced, for example, simultaneous malicious virtual machines on the server farm can reach other virtual machines or other server farms. Clients intersecting across different topographical zones can intensify attacks on other MEC's virtual servers. The virtual machine itself can be an attacker and other virtual machines hosted on the same system as an attacker and an attacker attack. [17]

5) End Devices Security: Recent client-side gadgets can affect several components of the biological community. However, the user may have an impact on the environment of a limited device. Client gadgets come as a vendor in a domain that is allowed to run. At the same time, there may be rebel clients who can break the revolution and perform some obscene training. For example, they can include fake properties or data. You may also be sending false information such as device reconfiguration and incorrectly supplied information about camera surveillance or incorrect information about vehicles. There are also some scenarios that may involve the service manipulation of the devices. For example, any broken device that has been added to a clustered environment can modify and manage the services in that cluster. [17]

Chapter 4

Proposed Authentication Method

4.1 Introduction

Authentication

The process of authentication verifies the user's identity. The traditional authentication process to identify the system to the user via a user name and password via allows validating their identity. Such as X.509 certificates, one time passwords (OTP) and the device as fingerprinting, there are ways to strengthen user authentication. These authentication factors can be combined to a combination of stronger. Federated identity such as corporate identity management (IDM) system that occurred in another domain using authentication services such as software-as-a service (SaaS) application for one domain allows a user to access the application. [18]

Authorization

Authorization authentication step follows. This step determines that the user is allowed to gesture. It was part of the application's permission to access control. Here, regardless of the user's location or application authorization policy of decentralization. Authorization is determined based on a user's identity, but in most cases, such as the title role or the user may need additional attributes. IV

4.2 Proposed Authentication Method

We are working about robust security in mobile edge computing (MEC). In cloud mechanism we get the basic architecture that is in bellow:

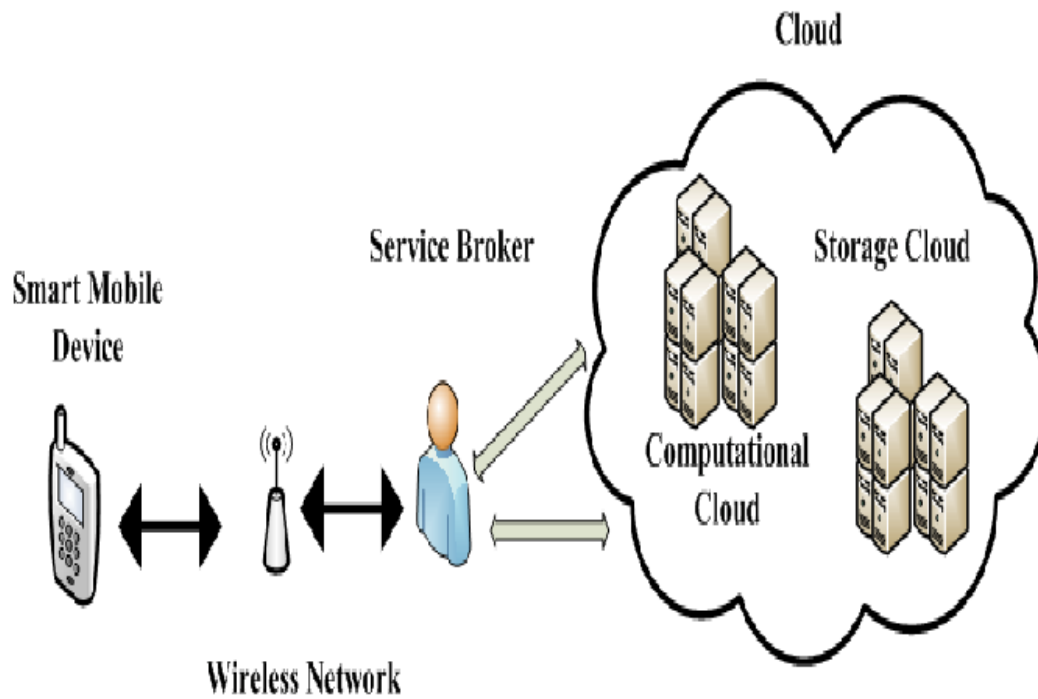


Figure 4.1: Connection End users to Cloud

From this figure we can see here the relation only between cloud and end user there in nothing between these two structures. Here end users directly connect with cloud without any authentication.

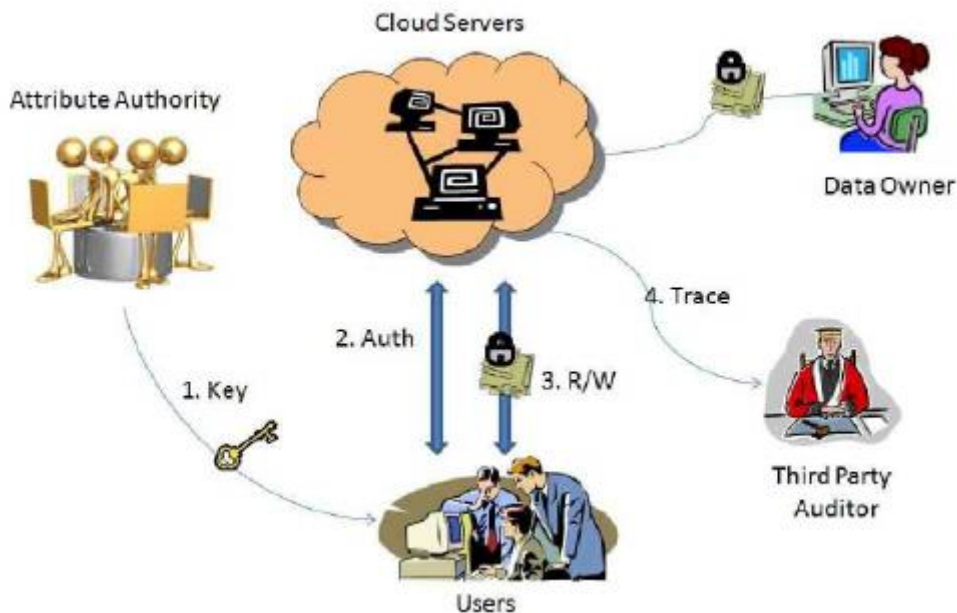


Figure 4.2: User Connects to Cloud server through Authentication server

Here we see the cloud server architecture with trusted third party authentication. Users always get two own keys. One public key and another is private key.

In 2010, Li et al. [19] Depicted a model to check a scalable channel access based on attribute encryption by preventing the illegal testing between colloid users not from the existing accessibility system based on attribute encryption. For this purpose, access control policies based on data attributes were defined and implemented. In addition, implementation model was implemented in this model by removing distortion removal and sending broadcast encoding method to support user and resistor use. The following figure shows the architecture of the given model of Li et al. (2010): In this model, user control was introduced by removing removal paths and transmitting encryption types for support of user bans and training. Figure shows the architecture of the given model of Li et al. (2010):

According to this figure, this confidentiality and celebrity core control show that it is efficient and practical in real-life cloud computing. Wang et al suggests an adaptive access control model through trust introduction into cloud computing and environments through roll-based access control methods for resource management and access control in communications weapons in cloud computing and environment. In addition, the proposed model includes a dynamic and trust-based access model to determine the security level and access control based on dynamic user authentication and effectively controls the user's generous behavior.

We are trying deploying this method in mobile edge computing (MEC) which is working as mini cloud. It is installed near to end user so that the users can feel the best cloud service. In previous chapter we see all types of attacks and problems in MEC. So it need to be robust the security in MEC.

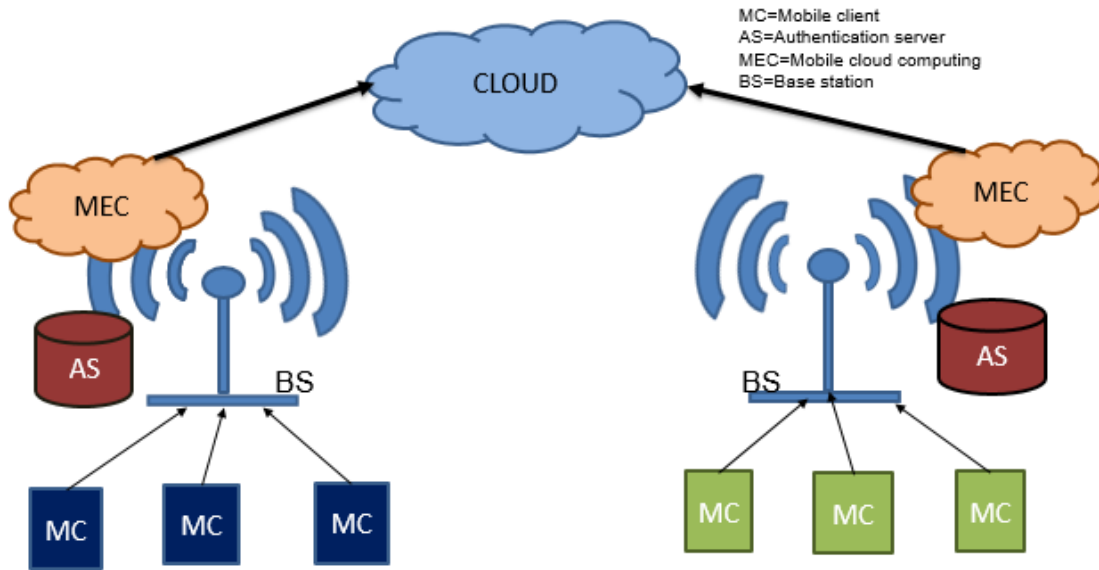


Figure 4.3: Authentication server include in MEC

In this figure we show our proposal in MEC architecture. Here we deploy MEC and Authentication Server (AS) in Base Station (BS). In this case the central AS assign some intelligence those AS which is deploy in BS. On account of those Mobile Client (MC) are connected with specified location based MEC those MC can also authorized by this mini audit. This also required the secured authentication in transferring any information or message and also required in secured mobility.

Here we are showing the flowchart about our architecture:

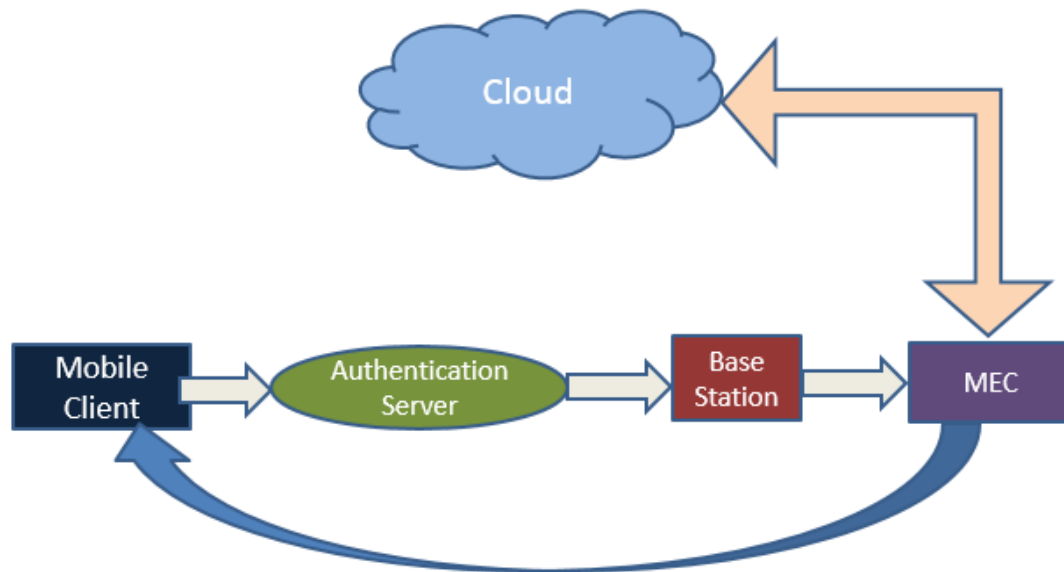


Figure 4.4: Flow chart of AS in MEC

Chapter 5

Result & Analysis

5.1 Experimental Setup:

For the simulation of the proposed method, Network Simulator Version 2 (ns-2) is been used. ns-2 is a discrete-event network simulator, targeted primarily for research and educational use. ns-2 is free software, licensed under the GNU GPLv2 license, and is publicly available for research, development, and use.

The ns-2 project is committed to building a solid simulation core that is well documented, easy to use and debug, and that caters to the needs of the entire simulation workflow, from simulation configuration to trace collection and analysis. Furthermore, the ns-2 software infrastructure encourages the development of simulation models which are sufficiently realistic to allow ns-2 to be used as a real-time network emulator, interconnected with the real world and which allows many existing real-world protocol implementations to be reused within ns-2. The ns-2 simulation core supports research on both IP and non-IP based networks. However, the large majority of its users focuses on wireless/IP simulations which involve models for Wi-Fi, WiMAX, or LTE for layers 1 and 2 and a variety of static or dynamic routing protocols such as OLSR and AODV for IP-based applications. Ns-2 also supports a real-time scheduler that facilitates a number of “simulation-in-the-loop” use cases for interacting with real systems. For instance, users can emit and receive ns-2-generated packets on real network devices, and ns-2 can serve as an interconnection framework to add link effects between virtual machines.

Figure 5.1 shows the experimental setup of Secured MEC with authentication server which is designed in ns-2. The hexagonal yellow shape is the MEC cloud server whereas yellow squares are authentication servers along with blue squares is the mobile nodes. Two scenarios are designed where one is the MEC with the proposed authentication server and another is conventional MEC.

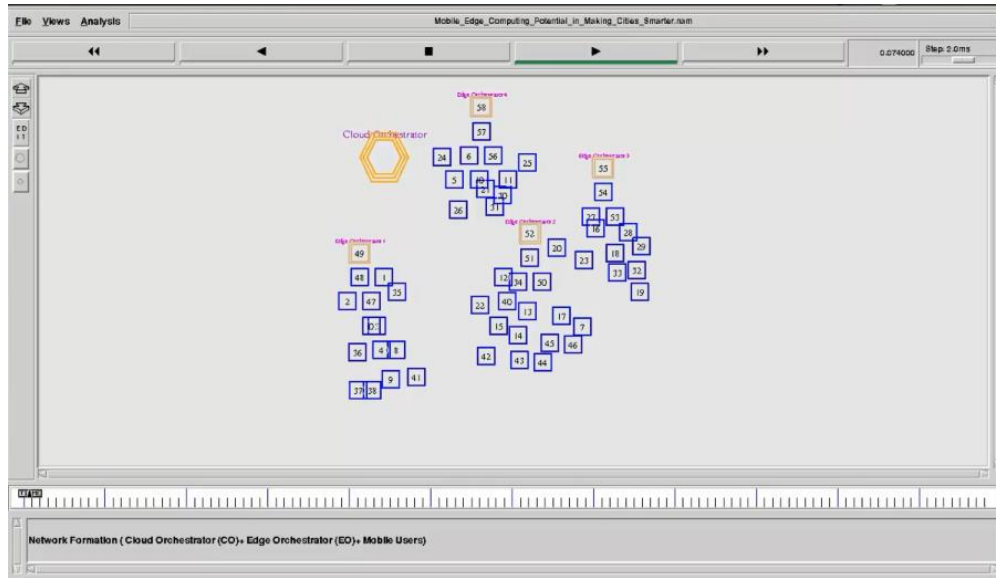
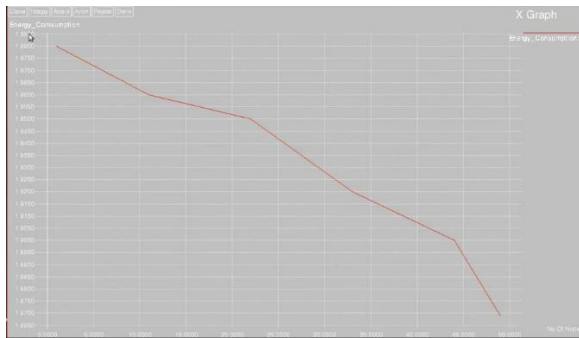


Fig 5.1: Experimental setup of MEC.

The energy consumption graph of proposed method and conventional method is illustrated in Fig 5.2. The X-axis of the graph denotes the number of nodes used in simulation whereas Y-axis of the graph denoted the energy consumption in milliwatt (mW). After observing the graph, it is seen that the proposed method has less energy consumption than conventional method with the increased node number. It means that less energy consumption means less interference.



(a) Energy Consumption (Proposed)

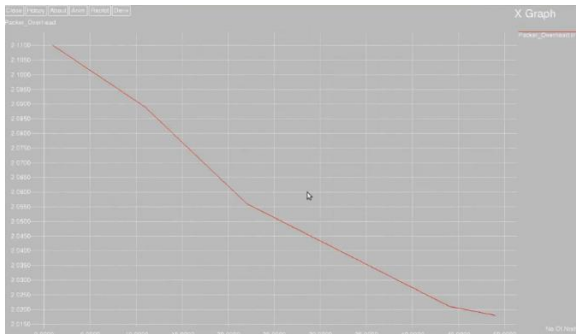


(b) Energy Consumption (Conventional)

Fig 5.2: Comparative Energy Consumption Graph.

The packet overhead graph of proposed method and conventional method is illustrated in Fig 5.3. The X-axis of the graph denotes the number of nodes used in simulation whereas Y-axis of the graph denoted the packet overhead in bytes. After observing the graph, it is seen that the proposed method has less packet overhead than conventional method with the

increased node number. It means that the authentication server reduced the unwanted packet which make the network congested.



(a) Packet Overhead (Proposed)

(b) Packet Overhead (Conventional)

Fig 5.3: Packet Overhead Consumption Graph.

Chapter 6

Conclusion

The use of modern-day Mobile edge computing has a great potential for using modern power supply, battery life and storage of electrical appliances. Authentication service in deploy is mainly the security robust in MEC system. For these reason the main AS can avoid the bottleneck in their system and additionally increased the secure mobility. We can reduce by this procedure Main-in-middle attack, DOS attack, location based attacks etc.

The MEC contributes to providing secure coverage of films to projects that require computer operating systems that have high bandwidth and ultra-low latency operating systems, especially in 5Gs. The preservation of the MEC can create natural resources including third parties for partnerships, acquisition agencies, software makers, OTT players, traders and many mobile phones.

Reference

1. Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected cloud computing environments: Challenges, taxonomy, and survey. *ACM Computing Surveys (CSUR)*, 47(1), 7.
2. Touceda, D. S., Cámara, J. M. S., Zeadally, S., & Soriano, M. (2015). Attribute-based authorization for structured Peer-to-Peer (P2P) networks. *Computer Standards & Interfaces*, 42, 71-83.
3. Ibrahim, M. H. (2016). Octopus: An Edge-fog Mutual Authentication Scheme. *IJ Network Security*, 18(6), 1089-1101.
4. u, S., Ratazzi, E. P., & Du, W. (2016). Security Architecture for Federated Mobile Cloud Computing. *Mobile Cloud Security*, Springer.
5. Bouzefrane, S., Mostefa, A. F. B., Houacine, F., & Cagnon, H. (2014, April). Cloudlets authentication in nfc-based mobile computing. In *Mobile Cloud Computing, Services, and Engineering (Mobile Cloud)*, 2014 2nd IEEE International Conference on (pp. 267-272). IEEE.
6. Yang, X., Huang, X., & Liu, J. K. (2016). Efficient handover authentication with user anonymity and untraced ability for mobile cloud computing. *Future Generation Computer Systems*, 62, 190-195.
7. McCarthy, D., Malone, P., Hange, J., Doyle, K., Robson, E., Conway, D., ... & Kastrinogiannis, T. (2015, May). Personal cloudlets: implementing a user-centric data store with privacy aware access control for cloud-based data platforms. In *Proceedings of the First International Workshop on Technical and Legal aspects of data privacy* (pp. 38-43). IEEE Press.
8. <http://www.rfwireless-world.com/Terminology/what-is-mobile-edge-computing.html> [Access time:10:00pm, Dec 15 18]
9. Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile edge computing: A survey. *IEEE Internet of Things Journal*, 5(1), 450-465.
10. https://en.wikipedia.org/wiki/Mobile_edge_computing#cite_note-VermesanFriess,2015-5 [Access time:11:30pm, Dec 15 2018]
11. https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf [Access time:3:23pm, Dec 16 2018]

12. <https://www.sdxcentral.com/edge/definitions/mec-standards/> [Access time: 3:40pm, Dec 16 2018]
13. https://lsalab.cs.nthu.edu.tw/home/publication/2018_SC2_MEC.pdf [Access time 8:00pm Dec 16 2018]
14. Mobile-Edge Computing Architecture: The role of MEC in the Internet of Things.. Available from: https://www.researchgate.net/publication/308767796_Mobile-Edge_Computing_Architecture_The_role_of_MEC_in_the_Internet_of_Things [Access time: 8:30pm Dec 17 2018].
15. Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). Mobile edge computing: Survey and research outlook. *arXiv preprint arXiv, 1701*.
16. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78*, 680-698.
17. Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile edge computing: A survey. *IEEE Internet of Things Journal, 5*(1), 450-465.
18. <http://www.iosrjournals.org/iosr-jce/papers/conf.15013/Volume%204/7.%2030-35.pdf> [access time:11:00am Dec 20 2018]
19. Ahmadi, M., Chizari, M., Eslami, M., Golkar, M. J., & Vali, M. (2015, May). Access control and user authentication concerns in cloud computing environments. In *Telematics and Future Generation Networks (TAFGEN), 2015 1st International Conference on* (pp. 39-43). IEEE.
20. (PDF) *Fog Computing Approach for Mobility Support in Internet-of-Things Systems*. Available from: https://www.researchgate.net/publication/325798491_Fog_Computing_Approach_for_Mobility_Support_in_Internet-of-Things_Systems [accessed Jan 04 2019 time 5.21 A.M].