A Comprehensive Comparison between Cloud Computing and Mobile Edge Computing

Farha Akhter Munmun, Adeeba Anis, Md. Shohrab Hossain

Department of Computer Science and Engineering, Bangladesh University of Business and Technology

***Abstract*: Cloud computing provides a user-convenient, low-expense, and powerful computing platform for sharing resources like online storage, applications, and software through the internet. But with the exponential growth of the Internet of Things (IoT) devices and massive amounts of private data in the network, the centralized and conventional architecture of cloud computing has become a bottleneck because of limited bandwidth and resources. At the same time security is also an open concern for cloud computing. Hence, Mobile Edge Computing (MEC) is an extended architecture of cloud computing that enables data processing and storing at the edge of mobile networks. Instead of having some unique features (distributed architecture, parallel processing, low latency), MEC has also brought some security threats and challenges. In this paper, a comprehensive comparison between cloud computing and MEC has been presented in terms of features and security threats. Also, the security mechanisms for handling the threats are analyzed.**

***Index Terms*: IoT devices, Cloud computing, Mobile Edge Computing, Security threats, Security mechanisms**

I. INTRODUCTION

With the advent of internet technologies, people have become much more dependent on smart computing devices. Over the last few years, the popularity of IoT devices is increasing explosively due to lower cost and user convenience. So, nowadays individuals or any kind of organization want such a high-performance and smart platform where they can have access to shared resources without acquiring them physically [1]. Therefore, the idea of cloud computing has emerged. Cloud computing is a distributed and parallel computing system containing a set of interconnected resources based on an agreement between the consumers and service providers [2]. With the latest and advanced characteristics of cloud computing like resource pooling, scalability, and large network access, the security and privacy challenges also increase. Moreover, direct and unauthorized access to the cloud makes it more vulnerable to threats. Also, the centralized architecture of cloud computing increases the average response time and jitter because of the large physical distance between the end users and clouds [3].

To solve the problem of the long delay, a new standard namely edge computing [4] has emerged. The first technology of edge computing has been introduced in 2009, which is cloudlet [5]. Although this cloudlet technology has been developed to extend mobile cloud services, it was inefficient due to its restricted WiFi coverage. On the other hand, MEC [6] is developed with better offloading technologies that can distinguish the network with high bandwidth and lower latency. In MEC architecture, the data is processed very close to the end-users, reducing the average latency and jitter. This property makes MEC most applicable for delay-sensitive applications. In recent years, some related technologies like mobile cloud computing (MCC) [7], [8], fog computing [9] also provide better user convenience. Instead of having many beneficial characteristics such as distributed nature, massive amounts of data processing power, high mobility support, location awareness, and low latency, privacy and security is still an open concern for MEC. Most of the small and smart computing devices are highly resource-intensive and it is quite challenging to implement any strong security algorithm without hampering their lightweightness.

The main objectives of this paper can be summarized as:

- An overview of the architecture of cloud computing and MEC is presented. The differences between their features are also described.
- A detailed analysis of the security threats and the consequences related to cloud computing and MEC is summarized.
- A comprehensive comparison between these security threats is pointed out.
- Some of the popular mechanisms for avoiding these threats are presented.

The rest of the paper is organized as follows: In Section II, background studies. In Section III, the state-of-the-art security threats of cloud computing and MEC are described. Section IV represents some of the popular security mechanisms. Finally, we have concluded the paper in Section V.

II. BACKGROUND

A. Cloud Computing:

According to the National Institute of Standards and Technology (NIST) [10], the final definition published of cloud computing is a combination of five essential characteristics: on-demand network access, shared pooling of resources, access of large networks, rapid expansion, and measured services. The basic architecture of cloud computing includes three layers and each of these layers provide different services such as: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a service (IaaS). Table I represents the services provided by these layers. In recent times four basic models are used for the deployment of the

cloud: i) Public cloud, ii) Community cloud, iii) Private cloud, and iv) Hybrid cloud. Table II provides a detailed description of these models. Fig. 1 shows the deployment models combined with the service models (SaaS, PaaS, and IaaS).

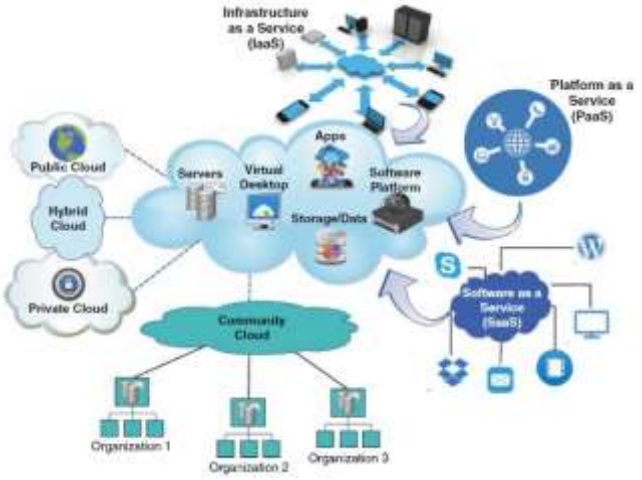

Fig. 1. Cloud computing services and deployment models [11]

B. Mobile Edge Computing:

The concept of MEC was first introduced by the European Telecommunications Standards Institute (ETSI) in 2014 and can be defined as a networking paradigm that merges the capabilities of cloud computing with cellular networks [12]. Improved application performance and reduced network congestion by connecting the end-users to the closest cellular network and bringing the storage capacity to the edge of network is the basic idea behind MEC. Worldwide many telecom operators such as DOCOMO, Vodafone, and Telecom Italia have benefited from MEC. Furthermore, many manufacturers, for example, Huawei, IBM, Intel, and Nokia Networks are additionally moving towards the normalization of MEC. MEC is basically a three-layer hierarchical architecture that occupies between mobile devices and the cloud. This three layer architecture includes the cloud server layer, the edge server layer, and the edge device layer hierarchically. Fig. 2 shows the three-layer architecture of MEC.

1) Cloud server layer: The cloud server layer consists of several data centers and the central cloud server. The primary responsibility of the data centers is to store a large amount of data generated by mobile and IoT devices. The cloud server maintains computation, authentication, and authorization.
2) Edge server layer: The edge server layer has multiple sublayers with various edge servers. The edge server performs the computational tasks and then sends the responses back to the

Fig. 2. Three-layer architecture of MEC.edge devices through different wireless interfaces.

3) Edge device layer: This is the lowest layer in MEC architecture. Each edge device performs the tasks of actuating, sensing, and controlling.

C. Feature Comparison of Cloud Computing and Mobile Edge Computing

The architectures and data processing of cloud computing and MEC are different and can not replace one another. Edge computing has been preferred by many organizations because of solving some issues of cloud computing. Some of the major differences between cloud computing and MEC are shown in Table III.

Table Iii. Major Differences Between Cloud Computing And Mec Features

Parameter	Cloud computing	MEC
Ownership	Private entities	Telecom companies
Storage capacity	Ample	Limited
Distance to end users	Large	Small
Deployment	Network core	Network edge
System management	Centralized control	Hierarchical (distributed) control
Location Awareness	No	Yes
Latency	High	Low
Network delay	High	Very low
Mobility	Limited support	High support
Security	Requires lower security plan	requires higher-level security

III. SECURITY THREATS

Security threat can be defined as a potential that can violate the security of any computer system and organization. In this section, some of the major security threats for cloud computing and MEC are explored. The security threats of cloud computing are classified into three main categories which include: data threats, network threats, and cloud environment security threats. Different categories of cloud

security threats and consequences are summarized in Table IV. Furthermore, the security threats of MEC are also divided into four main categories which include: virtualization infrastructure security, edge security, core network security, and user device security [12]. The consequences of these security threats are presented in Table V and the comparison between cloud computing and MEC security threats is shown in Table VI.

Table I. Cloud Service Models

Layers	Services
Software as a Service (SaaS)	This layer is known as the application layer. This layer allows the users to access applications running on the cloud without purchasing. Because of low expense, SaaS is very popular among business organizations. Salesforce.com, Amazon Web Services, Microsoft Office 365, Google Apps, Concur, Zendesk, Dropbox, and Slack are some of the popular applications that offer SaaS. Zendesk is a cloud-based service platform that processes thousands of customer's tickets daily. Google Apps includes Gmail, Google Drive, Google Docs, Google calendar, Google Meetings, and many other applications.
Platform as a Service (PaaS)	This is the middle layer and is also known as the platform layer. This layer provides an on-demand environment for users to develop or design specific applications. The services provided by the platform layer also include software development libraries and tools without any payment. SAP Cloud, Microsoft Azure, Heroku, AWS Lambda, Google App Engine, Dokku, Salesforce Lightning, and Zoho Creator are some of the popular PaaS providers.
Infrastructure as a service (IaaS)	IaaS is present in the bottom layer and is known as the system layer. In this layer, resources are combined physically or virtually and services are delivered in the forms of storage, network, or computational capability. VMWare, Amazon EC2, Sun Parascale, IBM Cloud, Vultr, and Digital Ocean are some of the popular IaaS providers.

Table II. Cloud Deployment Models

Models	Description
Public Cloud	The cloud architecture is designed in a way that the public can access the data center on a *"pay as you go"* basis. All the cloud resources such as storage and servers are owned, operated, and managed by any cloud service provider. This model is popularly used for providing online office applications and web-based emails. The advantages public cloud provides include lower expense, no maintenance, nearly unlimited scalability, and high reliability. One of the popular examples of public cloud is Microsoft Azure.
Private cloud	In private cloud environment resources are owned, operated, and managed by a specific organization on a private network. All the software and hardware are completely dedicated to the specific organization and thus make it more comfortable for the organization to maintain all the resources. Some of the advantages of private cloud are flexibility of customization, higher level of privacy, and control.
Community cloud	The physical infrastructure is owned, operated, and managed by a set of organizations called a community. The primary idea is to permit multiple users belongs to the community to share the same applications. This deployment model provides benefits to the community such as high availability, security, reliability, control, and convenience.
Hybrid cloud	Hybrid cloud combines public, community, and private cloud. Many business organizations prefer hybrid cloud due to its advantages of flexibility, cost-effectiveness, and easiness.

A. Threats in Cloud Computing

1) Data threats: Data is one of the most significant and valuable resources of any system and organization. With the increasing number of cloud users, the amount of data stored in the cloud is also increasing. Data can be generated in both client and server, transferred in the cloud, and stored in the cloud storage. Keeping data secured is one of the major challenges for attaining cloud security. Most of the security issues arise in cloud computing because customers have no idea about where and how the data are actually stored. Security threats can also arise due to lack of proper maintenance of cloud service providers. Two of the major data threats in cloud computing includes data breaches and data loss [13].
2) Network threats: The efficiency of cloud service mostly depends on how secure the network is and the users communicate with each other through the network. Most cloud-based organizations do not consider the security of the network as an important factor. That's why most cloud systems are vulnerable to different web browser attacks. Denial of Service (DoS) attacks and account hijacking are the common types of network threats.
3) Cloud environment security threats: The cloud environment is controlled and maintained by the cloud service providers. Many security threats are generated by the service providers in the cloud environment.

Table Iv. Consequences Of Cloud Computing Security Threats

Category	Security threats	Consequences
Data threats	Data breach	1. Leakage of sensitive data. 2. Access to adversaries in unauthorized way.
	Data loss	1. Deletion of data. 2. Erroneous data. 3. Storage system failure. 4. Natural disaster.
Network threats	Denial of Service (DoS) at-tack	1. Prevent legitimate users from accessing cloud services. 2. Delay in cloud operations and responses.
	Account hijacking	1. Stealing of user credentials. 2. Access of adversaries to user data and account.
	Phishing	1. Introducing malicious code into the user's PC. 2. Make the cloud server inaccessible to users.
Cloud environment security threats	Insecure interface	1. Third-party can get access to cloud services for weak APIs. 2. Violation of authentication. 3. Violation of access control. 4. Loss of data integrity.
	Malicious insider	1. Access of any third party to do unprivileged tasks with the help of an employee inside the

		cloud organization. 2. Leak of data with the help of any insider employee.
	Abuse of cloud services	1. Misuse of cloud services by the consumers. 2. Misuse of network addresses to create spam by malicious users.

B. Threats in MEC

1) Virtualization infrastructure security threats: A virtual infrastructure is more vulnerable to security threats because a change of any of its entities can affect the whole environment. This may occur DoS attacks, continuous reduction of data, and stolen of user's private data. Virtualization is the most important factor for edge computing and thus it's necessary to make the virtual infrastructure secure. For this reason, various methods are developed in [14] like network abstraction, network isolation, and Virtual Machine (VM) hardening.
2) Edge security threats: MEC reduces the network delay and jitter that occurs highly in cloud computing by replacing its server to the edge of the network. Due to this close connection with end-users, MEC is more vulnerable to security threats such as eavesdropping, man-in-the-middle attack, DoS attack, hijacking, etc. It is very much easy for any pernicious attacker to make the server inaccessible at the network edge by creating too many false requests. To avoid this problem, a round trip time-based method is followed that measures the time delay between the server and the user.
3) Core network security threats: The security of the core network is maintained by those organizations which include the user's sensitive information. For MEC end device is an important element in the whole system and an intruder can come as a user that can cause a serious disaster if false information is spread to the core of the network. An intruder can also provide bogus values to the sensors of the system.
4) User device security threats: The user device is also an important element in the whole system and the intruder can come as a user though the scope of this threat is limited. Any user device can be reprogrammed by any malicious third party to distribute bogus information to the network.

IV. SECURITY MECHANISMS

Providing security, especially the security of data becomes the most crucial challenge in cloud computing and MEC environment [21]. So, it is required to implement new mechanisms to make the total environment and data secure. Some of the security mechanisms to avoid these security threats have been presented in this section.

A. Security mechanisms in cloud computing

1) Defense mechanism against data breaches: Data breach in cloud environment is so significant that it ranks first in the Cloud Security Alliance's (CSA) 2019 list of the "Egregious 11" threats in cloud computing [15]. To avoid data breaches in cloud researchers implemented different techniques. Instead of storing plain/ original data in cloud data can be encrypted using any strong encryption algorithm. Unauthorized access can be prevented by:

- Making sure that each client can get to just their current circumstance and information and that other client's frameworks, information, and applications are imperceptible to him [16].
- Maintaining strong access password.

2) Defense mechanism against data loss: Providers should maintain a frequent backup of all data stored in the cloud that will be accessible in case of data loss. Providers should also make it transparent to the user what type of backup methods they are performing.
3) Defense mechanism against account hijacking: Account hijacking has also become a great threat in cloud environment. This can be avoided by implementing intrusion detection system (IDS) to detect malicious traffic in the network. Multi-factor authentication (MFA) is a great solution to avoid account hijacking.
4) Defense mechanism against DoS attack: The defense mechanism of a DoS attack is a combination of four steps which include: prevention, monitoring, detection,

Table V. Consequences of Mec Security Threats

Category	Security threats	Consequences
Virtualization infrastructure security threats	Distributed Denial of Service (DDoS) attack	Malicious virtual machine diminishes computational, network, and storage resources.
	Misuse of resources	1. Executes malicious programs in local or remote entities. 2. Continuous reduction of data.
Edge security threats	Man-in-the middle attack	1. Malicious adversaries take control of any section of the network. 2. Allows attackers to access users' private data. 3. Insertion of malicious data in such a way that is identical to the legitimate data.
	Service hijacking	1. Stealing of user credentials. 2. Access of adversaries to user data and account.
	Eavesdropping	1. Modification of data transmitting between two end devices. 2. Insertion/ deletion of data transmitting between two end devices.
Core network security threats	Rogue gateway	Malicious attackers deploy their own gateway
	Denial of Service (DoS) at-tack	1. Denial of service. 2. Legitimate users lose access to the core network.

User device security threats	Injection of information	1. Adversaries reprogram the user device to distribute fake information. 2. Provides bogus values to the sensors of the devices.
	Service manipulation	1. Adversaries take control of user devices. Manipulation of service outcomes.

and mitigation [17]. The prevention phase prevents cloud resources and services by initiating proper applications. The monitoring phase monitors necessary information about the hosts. The detection phase investigates the source traffic to check whether it is malicious or not. The mitigation phase takes necessary action against malicious traffic.

5) Defense mechanism against malicious insiders: It is very difficult to protect cloud data from malicious insiders. Separation of duties in the management layer and implementation of strong access control protocol can reduce this type of attack.
6) Defense mechanism against abuse of cloud services: Implementation of two methods can identify malicious users that include strict registration and validation process.

Table Vi. Comparison Between Cloud Computing and Mec Security Threats

Security threats	Cloud computing	MEC
Billing attack	No	Yes
Man-in-themiddle attack	No	Yes
Data breach and data loss	Yes	Yes
Account or service hijacking	Yes	Yes
Attacks in geographical location	No	Yes
Information flow manipulation	No	Yes
Service Manip-ulation	No	Yes
Eavesdropping	No	Yes
Provides bogus information	No	Yes

7) Defense mechanism against insecure interface and APIs: The cloud service providers must ensure that the interfaces and APIs are designed and developed by trusted designers and developers.

B. Security mechanisms in MEC

1) Identification and authentication: In MEC environment different data centers are hosted by different service providers. It depends on their choice as well as their budget. So, in MEC this is so important to identify and authenticate each connected device like end users, virtual machine services, MEC service providers. In [18], identity federation mechanisms and inter-realm authentication systems have been proposed for providing authentication.
2) Network security: Network infrastructure has a profound impact on MEC because if the infrastructure is not secured, the whole system will be at a risk of internal and external attacks. So, it's necessary to protect the protocols and technologies used by MEC such as WiFi, LoRa, Sigfox, etc [22]. It is still very difficult to maintain security mechanisms for MEC because attackers-initiated attacks like man-in-the-middle attacks and DDoS attacks to make the network vulnerable. In [19], [20], some defense mechanisms against DDoS attacks have been described.
3) Virtualization security: One of the main foundations to get a secure MEC paradigm is virtualization technology. Malicious elements can snatch the whole data center by getting access to virtual servers. Virtualized servers and physical servers hosted by them can be protected through strengthening the hypervisor, isolation policies, and network abstractions.
4) Data security: In MEC paradigm, the MEC server stores the user's data. Mobile users get access control which creates various challenges such as proper authorization and data integrity. Auditing methods should be maintained properly and on regular basis to check whether the data is properly kept in the cloud or not.
5) Data computation security: Another important issue for MEC is to make the data computation secure. To secure the data computation two techniques including data encryption and data verification are very much useful. A variable computing protocol can be used in case of computation verification. Another important security mechanism is data encryption. When the data is sent from the user end to the MEC servers, it should be encrypted and protected.

V. CONCLUSION

Cloud computing has made lots of benefits for its users including cost savings, configurable resources, and service affability. Though the benefits of cloud computing are clear, the centralized architecture of cloud computing becomes a primary obstacle to the wide-scale adaptation of clouds. However, MEC, the extended architecture of cloud attains lots of attention during the past decade due to bringing cloud services to the edge of a network and has some advantages over cloud computing like low latency, low bandwidth utilization, low expense, etc. Instead of having so many advantages, privacy and security are still an open concern for both cloud computing and MEC. In this paper, we have presented some of the common cloud and MEC security threats and the state-of-the-art security mechanisms. We have also compared the features and security threats of both technologies. These findings can be a guideline for the

network designers or engineers for further improvement in the existing security mechanism.

REFERENCES

[1] R. Choubey, R. Dubey, "A survey on cloud computing security, challenges and threats," International Journal on Computer Science and Engineering (IJCSE), vol. 3, no. 3, pp 1227-1231, 2011.

[2] R. Kaur, J. Kaur, "Cloud computing security issues and its solution: A review," IEEE 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp 1198-1200, 2015.

[3] M. Satyanarayanan, " A brief history of cloud offload: A personal journey from odyssey through cyber foraging to cloudlets, " GetMobile: Mobile Computing and Communications, vol. 18, no. 4, pp. 19-23, 2015.

[4] Y. Xiao, Y. Jia, C. Liu, J. Yu, W. Lv, "Edge computing security: State of the art and challenges," Proceedings of the IEEE, vol. 107, no. 8, pp 1608-1631, 2019.

[5] M. Satyanarayanan, P. Bahl, R. Caceres, N. Davies, "The case for vmbased cloudlets in mobile computing," IEEE pervasive Computing, vol. 8, no. 4, pp. 14-23, 2009.

[6] N. Abbas, Y. Zhang, A. Taherkordi, T. Skeie, "Mobile edge computing: A survey," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 450-465, 2017.

[7] S. Al Janabi, N. Y. Hussein, "The reality and future of the secure mobile cloud computing (SMCC): survey," International Conference on big data and networks technologies, Springer, pp. 231-261, 2019.

[8] P. H. Raj, P. R. Kumar, P. Jelciana, "Mobile cloud computing: a survey on challenges and issues," International Journal of Computer Science and Information Security, vol. 14, no. 12, p. 165, 2016.

[9] S .Yi, C. Li, Q. Li, "A survey of fog computing: concepts, applications and issues," In Proceedings of the 2015 workshop on mobile big data, pp. 37-42, 2015.

[10] NIST, Accessed on June 3, 2021. [Online]. Available: https://www.nist.gov/news-events/news/2011/10/final-version-nistcloud-computing-definition-published

[11] M. Liyanage, M. Ahmad, A. B. Abro, A. Gurtov, M. Ylianttila, "Cloud and MEC Security," A Comprehensive Guide to 5G Security, pp. 373397, 2017.

[12] A. Rasheed, P. H. J. Chong, I. W. H. Ho, X. J. Li, W. Liu,"An overview of mobile edge computing: Architecture, technology and direction," KSII Transactions on Internet and Information Systems (TIIS), vol. 13, no. 10, pp. 4849-4864, 2019.

[13] M. Kazim, S. Y. Zhu, "A survey on top security threats in cloud computing," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 6, no. 3, pp. 109-113, 2015.

[14] G. Pek, L. Butty´ an, B. Bencs´ ath, "A survey of security issues in hardware´ virtualization," ACM Computing Surveys (CSUR), vol. 45, no. 3, pp. 1-34, 2013.

[15] CSA Official Press Release, Accessed on June 30, 2021. [Online]. Available: https:https://cloudsecurityalliance.org/pressreleases/2019/08/09/csa-releases-new-research-top-threats-to-cloudcomputing-egregious-eleven/

[16] A. Poniszewska-Maranda, "Selected aspects of security mechanisms´ for cloud computing–current solutions and development perspectives," Journal of Theoretical and Applied Computer Science, vol. 8, no. 1, pp. 35-49, 2014.

[17] N. Agrawal, S. Tapaswi, "Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges," IEEE Communications Surveys Tutorials, vol. 21, no. 4, pp. 3769-3795, 2019.

[18] R. Roman, J. Lopez, M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, no. 48, pp. 680-698, 2018.

[19] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer Communications, no. 107, pp. 30-48, 2017.

[20] B. B. Gupta, O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment," Neural Computing and Applications, vol. 28, no. 12, pp. 3655-3682, 2017.

[21] O. M. AlMendah, S. M. Alzahrani, "Cloud and Edge Computing Security Challenges, Demands, Known Threats, and Vulnerabilities," Academic Journal of Research and Scientific Publishings, vol. 2, no. 21, pp. 156-175, 2021.

[22] F. Vhora, J. Gandhi, "A comprehensive survey on mobile edge computing: Challenges, tools, applications," IEEE Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 49-55, 2020.