All-in-Cloud: challenges and future expectations of AiC

Chenghao Li, Yanqi Pan, Yunqing He

ABSTRACT

With the development of the hardware and software of cloud computing, the evolution of the cloud has come to a new stage. Cloud makes it easier, cheaper, safer to store, transmit and process data. In recent years, technology keeps expanding to edge computing, fog computing and further. It is obvious that as time passes by, the occupation of the cloud devices compared with the local ones will keep increasing until the whole data becomes All-in-Cloud. However, rapid growth of the cloud comes with new problems concerning data privacy and security. This paper tries to focus on the development history of the cloud computing, discuss three cloud periods: cloud period, edge period and All-in-Cloud period. We analyze the challenges of data privacy and security in each period, and propose possible challenges and future expectations of All-in-Cloud. Finally, for better understanding, we apply our theory into some real cases to show concrete problems when they are facing All-in-Cloud situation.

Index Terms: Edge computing, Cloud computing, All-in-Cloud, data privacy and security, survey.

Directory

I. INTRODUCTION

1. Context

Cloud computing(CC): Cloud computing mainly deals with the problem of storing, computing, managing data online.[1] Usually, cloud computing is based on huge number of machines built together with powerful performance to provide data service to users.

Edge computing (EC): Edge Computing, which was mainly proposed to improve the Cloud Computing services in the era of IoT, is a complementation of Cloud Computing. And we define it as a series of technologies that allow data transmission, storing and processing happens at the distributed edge nodes as proximity to the end devices, end users and some sensors as possible. [2].

All-in-Cloud (AiC): All-in-Cloud describes the future of the cloud and the world. With the development of the cloud, more and more data become cloud data. The IT industry is moving their infrastructure into the cloud in recent years[3]. Finally, it’s obvious that the data will all be stored in the cloud which is called All-in-Cloud. Basically, it will take long to fully achieve AiC, but some industries and companies stepped forward and has achieved this recently[4], so All-in-Cloud is no longer an untouchable technology.

Cloud period: Cloud period describes the period when the cloud computing is mostly done in big data centers and provide with high performance computing to the users. In earlier days back to 1980s or earlier, the cloud technology was not widely used, so this paper doesn't include this period.

Edge period: Edge period describes the period when a large amount of cloud computing resource is applied to small devices covering much wider area compared to cloud period. In edge period, edge computing is in charge of the edge of the cloud computing, where

cloud computing is mostly done in small cloud, with relatively low performance but way more devices to do computing.

All-in-Cloud period: In All-in-Cloud period, all the data is stored, processed, computed in the cloud, and the cloud will cover all industries, making the world completely enter the world of Internet. All-in-Cloud period can be regarded as the final extension of the cloud period and edge period, but strictly speaking, this is impossible to achieve completely. But, if we've achieved most of these, we can assume that we are already in this period.

2. Motivation

Recently, the edge computing greatly expands the coverage of the cloud computing, which makes it available to provide detail device with explosive increase of the number of connected devices and edge nodes. It minimizes processing latency and the pressure of the cloud to provide stable cloud computing for the users. With the development of the advanced technology like 5G and IoE, the cloud is able to step forward to start its own revolution. 5G enables fast transmission of the cloud, enabling the cloud to cover larger area. Moreover, AiC can contribute to helping build the infrastructure of IoE (Internet of Everything), providing connected network and data platform for IoE.

AiC is never just a dream. Large cloud related companies have already made "AiC choice" and move their data to secure cloud platform. AWS declares that companies like Mike Chapple, Notre Dame have moved their all or most data on AWS[5]. For these companies, the cloud provides with much lower price, more stable service, more secure management.

While AiC is a great solution for companies, it's also a great approach for personal users to store their data. ICloud provides AiC service for personal users, as Apple has put all the photos, files and other data in the data from users' devices produced by Apple[6]. ICloud has made all the devices connected together, sharing data and creating new ideas, which helps build the data chain of the business, entertainment, creation.

3. Structure of the paper

In section 1, this paper explains the basic context in this paper, and talks about the background of the development of the cloud, and then shows the whole structure of the paper. In section 2, using the time dimension, we firstly give the give the development of the cloud, discussing the basic concepts of each period. And then we give the future expectations of AiC. At last, we propose the challenges of AiC. In section 3, we focus on some detailed cases to make the concepts of AiC clearer. In section 4, we will compare this paper with other related work and point out the contribution of the paper. Section 5 and 6 are the conclusion and reference parts.

II. The development of the cloud

The development of the cloud can be concluded into three periods: cloud period, edge period, All-in-Cloud period. In cloud period, the cloud is intended to solve the operation problems of huge project that ordinary compute can't handle in relatively small period, and provide unlimited resource and computing ability to users to create impossible things at the same time. In edge period, the cloud is intended to solve data related problems, with edge devices and edge computing set next to machines that produce data needed to be processed and stored in the cloud. With more effective data, the cloud is able to create much more accurate and useful results with less latency at the same time and as a result solve impossible missions that is limited to data. In AiC period, the cloud is intended to solve the world connection problems, with all the data stored and connected in the cloud, transferring the data problems into managing problems of the data. As a consequence, it makes the cloud completely become the infrastructure of the IT industry, replacing all the localized data to provide faster, more efficient, more powerful functions.

1.Cloud period

The cloud is built to overcome huge problems, which often takes long to get results when operated in a single computer. It sets an unaffordable barrier for small companies when they need to compute large amount of data, because high performance of the computing devices is very expensive to purchase and manage. However, the cloud completely changed the way the world works, with data stored, processed, managed in the cloud, systematic data centers built to provide professional support of the cloud and personal users operating big projects just using his own computer with the help of cloud computing. Moreover, the most important benefit that the cloud brings to people is its powerful performance and great flexibility, which makes one single person able to use the cloud to perform many challenging tasks. This greatly accelerates the development of IoT, big data and other IT areas at the same time. It greatly helps the development of the growth of the whole technology and the position of the cloud is fundamental and essential. This means if one technology can help improve the performance of the cloud, the technology itself is improving the whole IT industry. So, it's necessary to pay great attention to the cloud.

However, the more data we operate through the cloud, the more anxiety we suffer from the danger of privacy problems. Privacy problems should be the first to be taken into consideration, as it's the basic requirement when we send our data through the Internet. As the cloud is completely constructed on the Internet, the cloud is easier to be attacked and spread virus. Due to the fundamental position of the cloud, the problems of data privacy and security can't be ignored.

2.Edge period

To make most of the cloud, in recent years, edge computing has been growing rapidly. According to IDC, by 2022 over 40% of organizations' cloud deployments will include edge computing and 25% of endpoint devices and systems will execute AI algorithms [7]. On top of that, the devices related to the cloud computing keeps increasing in a very fast pace [8].

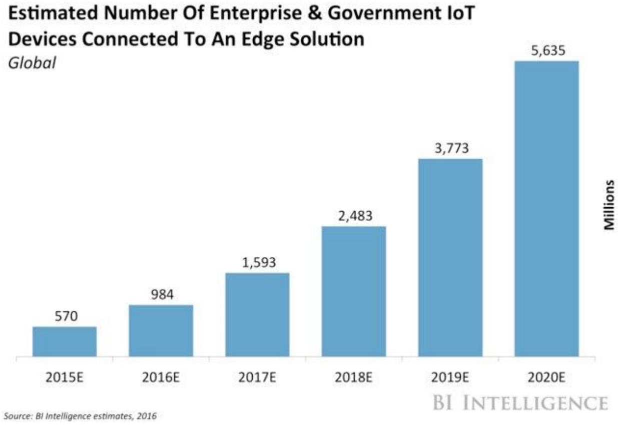
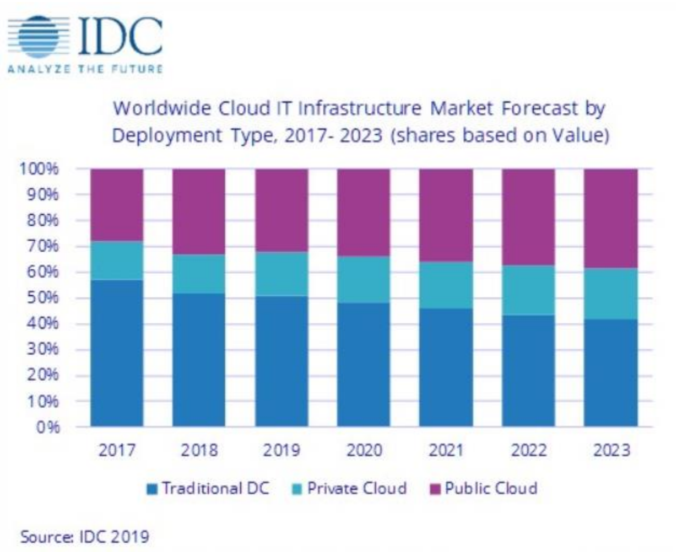


Figure1. EC devices[8]

However, there is one big problem about the cloud. As the cloud expands and more devices are connected online, data privacy and security are becoming more challenging and have to be solved. For example, in an ordinary family in the UK, there are about six connected devices placed at home[9], which is way too enough to monitor your daily life. It is obvious that if this family has suffered Internet attack and data leakage, the whole family is in great danger. So, the basic requirements for the cloud is to ensure that every device is secure enough. It’s getting a lot harder than before because of the explosive increase of the number of connected devices. Moreover, in the cloud center, it’s secure enough with professional security system, but in an ordinary family it’s not. This is completely different from period of cloud computing. The problems of edge computing are bigger and much more important. If we can’t solve these privacy problems, the development of the cloud will suffer and as a result influence the whole IT industry, because of the fundamental position of the cloud. In 2018, the new GDPR began to work, with huge amount of fine for those who break the rules, which showed great attention to the data privacy. We’ve been in a world with incredible need of data privacy. At the same time, we’ve been in the most dangerous world than ever before, with huge number of cases of data leakage, and privacy problems.

3.AiC period

Recently, the cloud has met its revolution, which helps IT companies move the whole data to the cloud. Because the traditional data center has some problems due to its hardware structure. For example, the traditional data center is often placed together and managed in a certain system. When this data center suffers unexpected attack or disaster, the whole data center may face the danger of data loss, the shutdown of the operating system. Often, to avoid this kind of problem, in addition to safety management, strict access control and other management approaches[10], there is no way else to minimize the danger to the trusted level unless the data center stores an copy in other places. However, the cost is relatively high. Moreover, the data center is always put near the owner, which limits the data center. Compared to the traditional data center, the scalability of the cloud is much bigger, and its data center locates in many positions and are not limited to the location of users. With less expense and more security management of the data, the cloud has unique advantages compared with traditional data centers. Consequently, the market sharing of the cloud keeps increasing, and will overtake the market sharing of the traditional data center in about 2020, according to IDC[11].



Source: IDC 2019

Figure2. Cloud infrastructure market sharing[11]

Until now, it’s still unclear how the All-in-Cloud is like, but it’s certain that we should get ahead to discover the possible challenges of AiC, and try to create the structure of it.

III. The newest technology of the cloud: Today’s AiC

With the improvement of Cloud Computing (CC) and Internet of Things (IoT), we are getting into a post-cloud era [12]. There will be numerous data generated by almost everything in our daily life to be transmitted, stored and processed. However, CC can't handle with all these data with very short response time which is exactly some IoT applications require[12]. In that case, Edge Computing (EC) emerges. In this section, we firstly overview the basic concepts related to the EC (Part 1), and after that, we list the advantages of current cloud structure (Part 2), and the next, we conclude the challenges of privacy and security problems in current cloud (Part 3),we make a brief conclusion of differences and commons between CC and EC (Part 4), and then we can be able to propose our ultimate goal: The future expectations of AiC based on that comparison.

1. Basic concepts

In [13], Wazir Zada Khan et al. showed us a structure of Edge Computing model, telling us how edge computing works. Figure 3 indicates the modern mechanisms of Edge Computing.

At present, cloud service is not only a kind of distributed computing, but also the result of mixed evolution and leap of distributed computing, utility computing, load balancing, parallel computing, network storage, hot backup redundancy and virtualization. And figure 3 indicates the current cloud computing architectures.

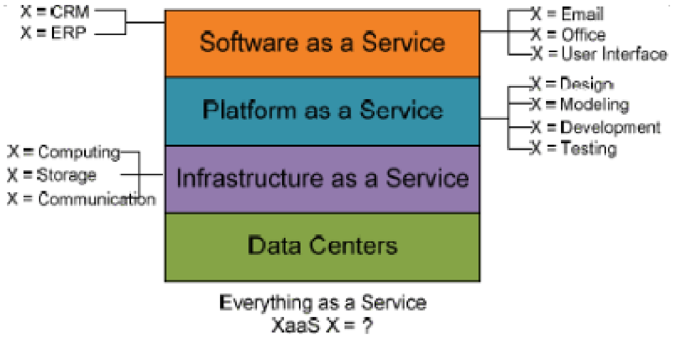


Figure 3. current cloud computing architectures [32]

Most clouds are built on top of data centers, which provides infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Figure 4 shows the hierarchical view of cloud computing.

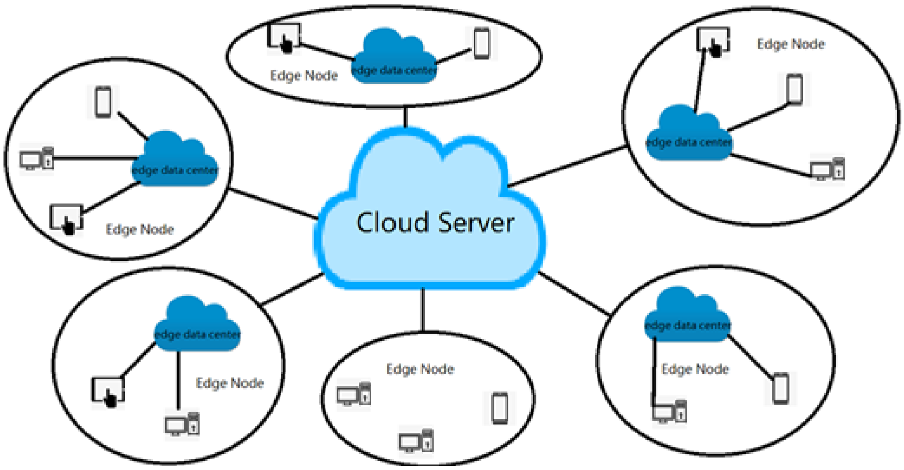


Figure 4. modern mechanisms of Edge Computing

Here, as the structure of modern cloud is similar to several years ago, we only list some models of the edge computing.

Fog computing. The concept was once proposed by Cisco. In their white book, they defined fog computing as a new strategy to connect more things to network, secure the data producers as well as secure the data transmission from the edge of network to the cloud servers, besides, handle with the heterogeneous data efficiently [14]. In other word, the fog computing provides low-latency and computation offloading services [15] to the end devices, end users and some sensors by deploying substantial distributed computing and storage resources such as routers and switches as proximity to the end devices, end users and some sensors as possible.

Cloudlets. Similar to the fog computing, cloudlet models are also deployed nearby the end devices, end users and some sensors. In [16], Satyanarayana et al defined the cloudlet as a trusted, resource-rich computer or cluster of computers that's well-connected to the Internet and available for use by nearby mobile devices. The difference is that fog computing emphasizes the data processing in the local area network, however the cloudlets put the data processing and storing inside the devices.

Mobile Edge computing. In [17], A. Ahmed et al gave their definition on Mobile Edge computing, that: "Mobile Edge Computing is a model for enabling business oriented, cloud computing platform within the radio access network at the close proximity of mobile subscribers to serve delay sensitive, context-aware applications". Similar to the above two, MEC is also deployed at the edge of networks, close to the end devices, end users and some sensors. According to the definition, the unique characteristic of MEC is its mobility support, and that's really a step forward in the AiC progress we'll discuss later. Table 1 concludes the basic concepts of EC.

Features Edge	Latency	Jitter	Geographic Position	Mobility Support	Concept Emphasis	Reference
Fog Computing	Low	Low	Distributed At the edge of networks	No	Data processing happens at local area network	[14][15]
Cloudlets	Low	Low	Distributed At the edge of networks	No	Data processing happens at most in devices	[16]
Mobile Edge Computing	Low	Low	Distributed At the edge of networks	Yes	Data processing happens at most in devices	[17]

Table 1 conclusion of basic concepts of EC

2. Advantages of current cloud structure

For cloud computing, there are three main advantages: supercomputing power, huge storage space and environmental protection. The processing power of cloud computing can rival that of supercomputers. Cloud computing allows users to experience speeds of 10 trillion calculations per second, which helps them search and analyze information. Cloud computing can also provide a very large amount of data storage space, which does not require the user to deploy any hardware costs. Finally, cloud computing can save users from worrying about the consequences of deploying IT products that will be eliminated from the market, reduce the energy consumption of the whole society, and help solve a series of problems such as environmental protection.

When it comes to IoT, data transmission latency, data security and privacy, data processing/analysis are always the main elements we should take into considerations. Nonetheless, in the conventional CC-based IoT, we generate a large number of data in our daily life, and all these data are needed to be sent to the cloud, which could cause lots of bandwidth usage but also high-latency data transmission between the cloud server and the end devices; besides, due to the long transmission distance from end devices to the cloud server, the data is easily attacked by malicious adversaries half on the way of the cloud server, apart from that, the cloud server is a highly centralized data center, hence once it was controlled by skillful adversaries, then a mass of data storing on the cloud server collected from anywhere might suffer from security and privacy leakage problems which totally do harm to thousands of cloud-use clients. In that case, data security and privacy seem to be fragile in the conventional CC-based IoT; lastly, due to data processing/analysis happens on the cloud server, so the management of cloud server would be crucial. There are some internal adversaries who abusing of their privileges to check or modify the data on the cloud, and there are also some external adversaries who gain their privileges by utilizing the management or policy leaks. Nowadays, In the EC-based IoT, things get a bit change.

- *Fast and stable data transmission*

  As mentioned before, EC is a series of technologies enabling data transmission, store and processing happens at the edge nodes as proximity to the end devices, end users and some sensors as possible. Obviously, the main feature of the EC is proximity, which means that the distance from the end devices to the edge nodes is short, and that contributes low-latency, low-jitter, low packet losses and high bandwidth to the data transmission, all of which are valuable for some applications, such as AR and VR, they both need offload computation to the edge nodes with a low-latency demand. [18]
- *Data security and privacy improvement in macro view*

  Compared to completely cloud computing, EC provide a way to process the data generated by things at the edge nodes as close to the end devices, end users and some sensors as possible. Short distance not only means the low-latency but also means that malicious adversaries have a fewer chances to attack the data during their transmissions to the edge nodes. Besides, the data transmitted to the cloud server via the edge nodes can be masked or encrypted by the edge nodes. In that case, the security and privacy of sensitive data is guaranteed at a high probability in a macro view.

- *Flexibility of data processing*

  In the CC-based IoT, users only process their data on the remote cloud server or totally local devices. In EC-based IoT, the delay sensitive part of application can be executed on the edge nodes whereas the delay tolerant compute intensive part of application can be executed on the cloud server [17]. In that case, the data processing becomes flexible. Since the edge nodes have limited computation and storage sources while the cloud severs 's is unlimited, besides, the edge nodes have low-latency data transmission which is beneficial to real-time applications while the cloud server can't provide such real-time services, users can balance the features to process their data more flexibility

3. Challenges of security and privacy problems

In cloud period, the main challenges are from three basic models of the cloud, in which the SaaS is the most popular one for personal users. In the SaaS model, the user's data is stored in the cloud server, that is, under the SaaS model, the user loses absolute control over the sensitive data. In this case, internal intrusion is very likely to occur, which may lead to the leakage of sensitive user information and other issues. At the same time, the multi-tenant nature of cloud computing means that the data of different users are all stored in the cloud environment, and malicious users can access other tenants' sensitive data stored in the cloud environment through application vulnerabilities and bypass security checks [38].

In edge period, EC lets the data transmission, store, and processing happen as proximity to the end devices, end users and some sensors as possible. However, since the EC is a complementation of Cloud Computing, some challenges of Cloud Computing are inherited. In the top layer, cloud sever, which can be able to receive the data coming from every edge node, can be vulnerable, adversaries can provide wrong services through the central cloud server; in the bottom layer, edge layer, where edge data center could be also targeted, besides, the EC-support technologies are diverse, but some of them are unsecured, such as Wi-Fi; apart from these, common network attacks are also challenges we are facing with. In this subsection, we categorize these challenges into three different data infrastructures. Data Transmission Infrastructure, which describes the challenges of security and privacy problems when the data is transmitted between end users and edge nodes as well as edge nodes and cloud server. Data Store Infrastructure, which describes the challenges of security and privacy problems when the data is stored at the edge nodes and on the cloud server. Data Processing Infrastructure, which mainly describes the problems of management leaks at the edge nodes as well as on the cloud server when the data is processed, and that might lead to challenges of security and privacy problems. Figure 4 concludes the structure of this subsection.

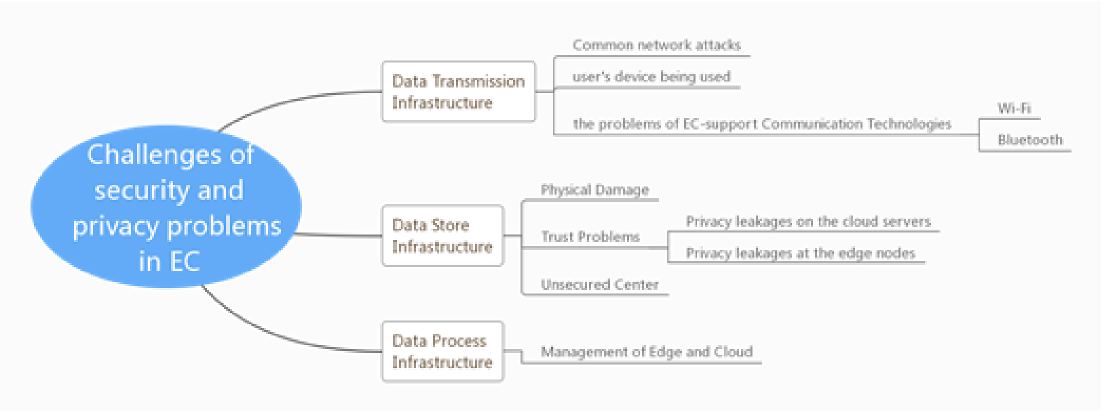

Challenges of security and privacy problems in EC
Data Transmission Infrastructure
Common network attacks
user's device being used
the problems of EC-support Communication Technologies
Wi-Fi
Bluetooth
Data Store Infrastructure
Physical Damage
Trust Problems
Privacy leakages on the cloud servers
Privacy leakages at the edge nodes
Unsecured Center
Data Process Infrastructure
Management of Edge and Cloud

Figure 4.
Conclusions of the structure of challenges of security and privacy problems in EC

3.1 Data Transmission Infrastructure

As aforementioned, with the EC models, data transmission welcome to a revolution – low-latency, low-jitter, low packet losses and high bandwidth. And also, fast transmission gives a fewer chances to malicious adversaries to attack the data half on the way of the edge node. However, there are still some potential challenges of data transmission – many common network attacks involved, users' devices being utilized and communication technologies security counts.

Common Network Attacks. Though unlike CC, EC decreases the scope of cyber-crime [17] by transmitting, storing, and processing data at the edge nodes, the common network attacks such as DoS and Man-in-the-Middle Attacks can disturb the work of EC as well. For example, if the edge data center is attacked by DDoS, then the data edge center will have lots of bandwidth and system sources being wasted, in that case, the data edge center can't response to the users' data, and it can't provide services for users as well, what's worse, when the system crashes, the data on the edge data center might be lost. Though, note that the crash of the edge data center only influences the users nearby it, for most of users, they don't want such situations happen to them.

Users' devices being utilized. Users' devices play an important role in providing data and participating in the EC ecosystem. Nonetheless, at the same time, users' devices are also potential weapons to attack the EC ecosystem. For example, once the malicious adversary takes the control of users' devices, then he can be able to disturb the ecosystem of EC. However, thanks to the EC models, such attack can only influence the immediate surroundings proximity to these utilized devices. In [17], Rodrigo Roman et al. proposed two threats models about users' devices.

EC-support Communication Technologies. The transmissions between the edge nodes and the end services are diverse. Such as Wi-Fi and Bluetooth, they are both communication technologies that support the transmission in EC ecosystem. However, there are also some security challenges we should face with. For the Wi-Fi technology, password leakage, directed information tampering and etc.; as for the Bluetooth technology [17], Bluebugging, Bluesnarfing and BlueSmack and etc. are also open challenges.

3.2 Data Store Infrastructure

As stated earlier, the data generated by end users, end devices and some sensors will be stored either at the decentralized edge nodes or on the centralized cloud servers which might lead to a series of open challenges of security and privacy. For the cloud servers, vulnerability, trust problems and etc.; for the edge nodes, damages caused by physical or cyber-attack, and also trust problems too. In that case, we must take several conditions into considerations.

Physical damage. Physical damage could happen to not only the edge nodes, but also the cloud severs. Though for the cloud servers, there's a little possibility being attacked physically, natural disaster should also be listed. As for the edge node, due to its special geographical position – proximity to the end devices, end users and some sensors – it is easily attacked by local people.

Trust problems. For the cloud servers, due to its characteristic of centralization, the service provider should be trusted third party. As for the edge node, it's decentralized in a macro view, comparing to the cloud. But it is indeed a centralized data center at the edge, in a micro view, which integrates the ability of data transmission, storing and processing. Besides, in [20], the edge nodes are mostly deployed without strict protection and monitoring, thereby facing many kinds of threats. In that case, privacy leakages, loss of data and etc. leaves a primary challenge.

Unsecured Center. No matter the cloud servers or the edge data center, they all have high probabilities to be targeted by skillful adversaries. For the most of cloud servers, the probability of successful attack is low, because cloud servers are protected through various means. However, as for the edge data center, as aforementioned, they are mostly deployed without strict protection and monitoring. In that case, such edge data center is really vulnerable and unsecured. Besides, one adversary even can be able to deploy his own malicious center, which could bring a series of security and privacy challenges.

3.3 Data Processing Infrastructure

As aforementioned, the data generated by the end devices will be processed at the edge nodes. In such case, it's more than important to assure the security of data processing which happens at the edge nodes. However, if the edge node mismanaged or the edge node had some internal adversaries with enough privileges can be able to modify the data, then the process happening at the edge nodes is unsecured. For example, once adversaries took the control of certain sections of the edge data center either by privileges escalation or by abusing of his own privilege as a legitimate administer, as a result, they can launch a several types of attacks, such as DoS or directed data modifying, etc. In that case, data privacy and security will suffer. [17]

4. Comparison: CC vs EC

Since the EC is a complementation concept of CC, they not only have lots of commons, but also a bunch of differences. In this subsection, we'll make a comparison through the data transmission infrastructure, data store infrastructure and data processing infrastructure. Table 2 concludes the comparison between CC and EC.

Data transmission infrastructure. In this infrastructure, geographical position should be considered at first. For the CC, cloud data centers have been sited where land and other costs are low, which means they tend to be far from population or industrial centers [21]; as for the EC, the edge nodes are deployed at the edge of networks, as proximity to the end devices, end users and some sensors as possible. Then, based on the different geo-position, CC tend to be high-latency, high-jitter and highly probable loss of packets while EC tend to be low-latency, low-jitter and seldom packets loss. When the data is transmitting, however, the CC and EC both suffer from the common network attacks such as DoS, Man-in-the-middle attacks and etc. As for EC, it also suffers from the EC-support Communication Technologies such as unsecured Wi-Fi and Bluetooth attacks and the problems that users' devices being utilized to disturb the ecosystem.

Data store infrastructure. In this infrastructure, storage capacity is a shortage of EC comparing to the CC since the EC has limited storage while the CC has unlimited one. Apart from storage capacity, CC is a highly centralized model while EC is a decentralized model in the macro view, which means that EC suffers less security and privacy problems than CC in such view. However, EC suffers more security and privacy problems than CC in the micro view, due to its proximity to the population, it might be attacked by local adversaries physically, which might unlike happen to CC.

Data process infrastructure. In this infrastructure, computation power comes first. As aforementioned, EC's computation power is limited while CC's is unlimited, which means that CC has advantages on fast computing. Apart from the computation power, EC and CC both suffer from management leaks such as privileges scalation or abusing of privileges or so on, which might bring a terrible scenario to the whole ecosystem.

	Comparison Points		CC	EC	Reference
Data Transmission Infrastructure	Latency/Jitter/Packet loss		High/High/High	Low/Low/Low	[15][16][21][22][23][24][25]
	Geographical Position		1.Far from end devices, end users and some sensors 2.Small quantity	1.Proximity to end devices, end users and some sensors 2.Dense quantity	[15][16][21][22][23][24][25][29]
	Open Challenges		Common network attacks	1.Common network attacks 2.Communication technologies problems 3.Users' devices being utilized	[18][26][27]
Data Store Infrastructure	Storage Capacity		Limited	Unlimited	[30]
	Centralization	Macro View	Centralized	Decentralized	-
		Micro View	Centralized	Centralized	-
	Open Challenges		1.Unsecured Cloud Center 2.Privacy Leakage	1.Unsecured Edge Data Center 2.Privacy Leakage 3.Physical Damage 4.Efficient Encryption Algorithms	[18][20][26] [27]
Data Process Infrastructure	Computation Power		Limited	Unlimited	[30]
	Open Challenges		1.Privileges scalation 2.Abusing of Privileges	1.Privileges scalation 2.Abusing of Privileges	[27]

Table 2 Comparison between EC and CC

IV. AiC: The future of the cloud

1. Structure of AiC

As for EC, we define it as “a series of technologies that allow data transmission, storing and processing happens at the distributed edge nodes as proximity to the end devices, end users and some sensors as possible.” The concept of EC is a complementation of CC, as EC decentralizes the cloud servers by deploying a series of edge nodes at the edge of networks. Figure 2 shows the basic structure of EC, from which we can tell that edge nodes include an edge data center and a bunch of different devices or sensors. (a small part of edge nodes has no edge data center due to the computation happens completely in the devices)

With the development of hardware and software, we’re stepping into a new era – Internet of Everything (IOE) [31]. A box, a towel, even a little toothbrush, all of that should be considered in such background, which means the data to be transmitted, stored and processed increase exponentially. In that case, the demand of low-latency, data privacy and security, rapid-computing will reach to a new level. Conventional EC model is clearly unable to meet the needs of such level. In that case, based on the above survey, we extend the concept of EC as AiC to satisfy the needs of such background.

Different from EC, AiC should be composed of countless powerful computation, storage-rich nodes to be able to carry numerous things. Besides, the distribution and connection of these should be considered in more details. We’ll make a recursive definition describe the AiC. To propose our definition of AiC, we first introduce some concepts.

Tiny edge data center: We define the tiny edge data center by utilizing the concept of tree. Tiny edge data center is almost same as the edge data center, the difference is that if edge data center is a root, then the tiny edge data center is a node.

End node: We define the end node as a totally privacy area, which includes a tiny data center and a bunch of devices and sensors. In this area, all the devices and sensors are trustable, they all connect to the tiny edge data center, controlled by client himself. Tiny edge node. We define the tiny edge node as an edge node which contains a tiny data center and a bunch of tiny edge nodes.

Finally, we can then give our definition of AiC. AiC is an EC-like model where the edge node contains an edge data center which connects to a bunch of tiny edge nodes, at the same time, the tiny edge node contains a tiny edge data center which connects to a bunch of tiny edge nodes or end nodes, continuing cycle until the tiny edge data center connects to the end node. Figure 5 shows the basic structure and concepts of AiC.

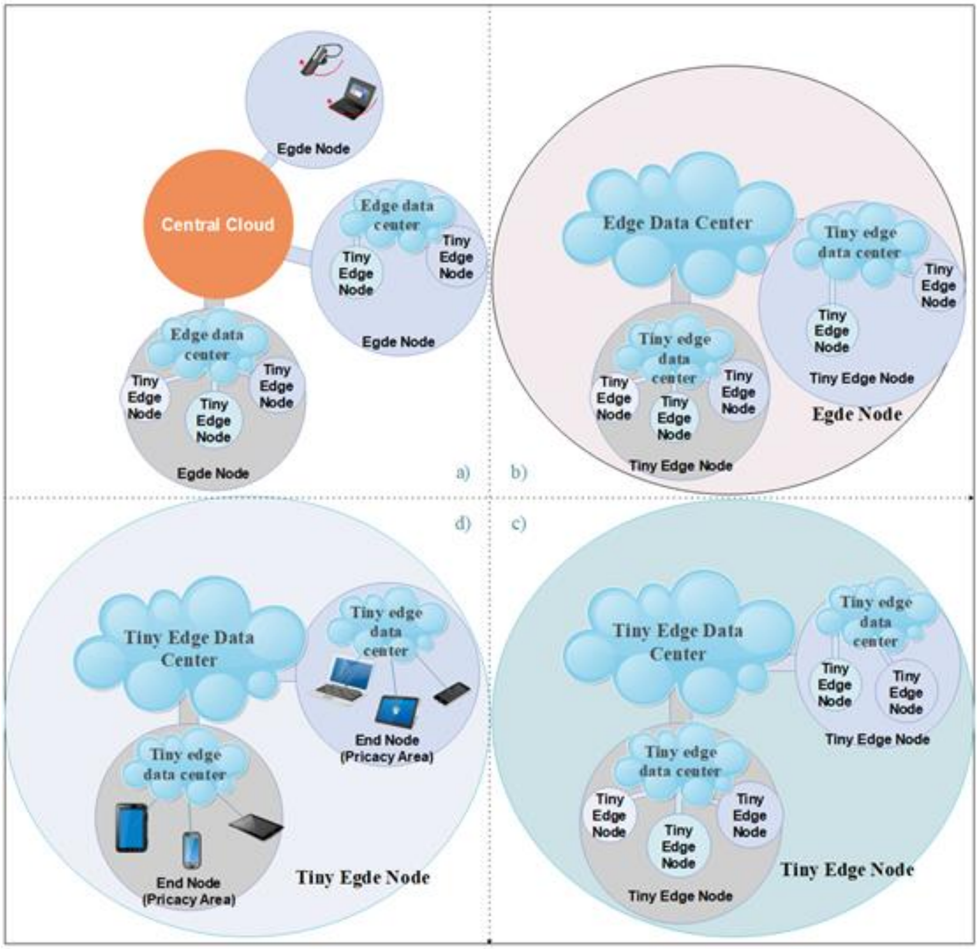


Figure 5. basic structure and concepts of AiC: a) The EC-like model b) The Edge node c) The Tiny edge node (A recursive definition) d) The End node

2. Application

AiC helps many industries construct their own powerful and comprehensive data structure and enables them to create impossible projects [37]. AiC makes it possible for IoT to become IoE, with flexible computing ability from small edge nodes to cloud data centers. Moreover, AiC helps build smart city with endless coverage of connected devices to provide data support for management of the city.

The AiC also faces new challenges of application, as new technology of managing the structure of AiC hasn’t been proposed yet, but the basic structure already shows the potential of the AiC in speed, coverage, security. AiC isn’t an approach to solve certain problems or certain projects. It’s a kind of infrastructure related revolution, which increases almost all the abilities from every dimension of the cloud, which means wider applications in all areas.

3. Challenges

As AiC expands the cloud nodes, mostly smaller ones, which greatly changes the way the cloud works, so some challenges of AiC are quite different from old versions of the cloud. Here, we list four essential challenges of AiC: privacy leakage, Protocols of standardization, Cost of deployment and chain reaction.

3.1 Privacy Leakage

On account of EC's decentralization in the macro view, EC increases the data security and privacy protection ability in such view [12]. However, in the micro view, as aforementioned, EC is highly centralized, it might suffer bigger problems. As for AiC, we defined the end node, which represents a privacy-safe area, in this area, all the devices and sensors are trustable, they all connect to a tiny edge data center, controlled by user himself. In that case, all the individual data transmission, store and processing happens in this trustable area, which means that no matter in the macro view or in the micro view, AiC is totally decentralized for users, so the TPA trust problems [33] are completely solved.

However, totally decentralization also brings some privacy leakage problems. Once a device was controlled by a malicious adversary, then he can take control of all the sensitive information by accessing the privacy area of device's owner. Nonetheless, note that the scope of such attack is limited, which only influences the things in the range of one small end node. Besides, there are still many approaches to protect or prevent such attack, such as fingerprint recognition [34], monitor detection and etc.

3.2 Protocols of standardization

As aforementioned, in the EC background, the edge data centers are deployed mostly by the same company that holds the central cloud sever, largely because the number of edge nodes aren't too many. However, in the AiC background, there are countless tiny edge nodes, which means only one company can't deploy them all, so more than one company takes part in maintaining the whole work of AiC ecosystem. In that case, AiC urgently demand some efficient protocols of standardization, including new standardization of data transmission, data store, data processing, data encryption, data decryption and so on. We survey some of common protocols in the past works.

The Hypertext Transfer Protocol (HTTP). HTTP is a stateless application level protocol for distributed, collaborative, hypertext information systems which is designed not only to hide the details of how a service is implemented by presenting a uniform interface to clients that is independent of the types of resources provided, but also designed for use as an intermediation protocol for translating communication to and from non-HTTP information systems. HTTP proxies and gateways can provide access to alternative information services by translating their diverse protocols in to a hypertext format that can be viewer and manipulated by clients in the same way as HTTP services. [35]

Transmission Control Protocol (TCP). TCP is used to interconnect network devices on the Internet. The TCP performs the handshake between the network devices to establish a socket. The socket remains open during the communication. The source TCP converts the data into packets and sends to the destination TCP. The TCP performs acknowledgment for the successful delivery of the packets. If a packet drops on the way, the source TCP resends the packet. [36]

3.3 Cost of deployment

In the earlier EC background, the edge data centers were deployed directly by the same company that holds the cloud server, users needn’t have to do anything then they can benefit from EC. However, in the AiC background, there are countless nodes deployed from end nodes to the central cloud server. In that case, AiC needs users to deploy a tiny data center themselves due to the number of the end nodes. Then, the cost of deployment is taken into considerations. How to decrease the cost of deployment, which might include cost of time, cost of money, cost of physical space, cost of man source and etc.

3.4 "Chain Reaction"

In the AiC background, the whole cloud framework presents the status quo of star emission, and data transmission exists between two adjacent cloud data centers, which brings new challenges to the security protection of the whole system.

If the edge/tiny edge data center at the edge/tiny edge node is not strong enough to deal with malicious data intrusion or network attack and once these nodes are maliciously invaded, they can pass the wrong data to not only their lower level tiny data centers, but also their upper level edge data center /tiny edge data center/cloud server which in turn can pass the wrong data to all its lower level edge/tiny edge data centers. As you can imagine, if this process is repeated, then the whole AiC ecosystem will be in danger. However, it is not difficult to find that what causes the whole AiC ecosystem to be exposed is only the intrusion of some edge/tiny edge data centers. Therefore, AiC ecosystem is not only vulnerable, but also each attack cloud lead to produce more and more serious “Chain Reaction”. This poses a higher challenge to the safety of the whole AiC ecosystem. Figure 6 shows the cloud chain before attack, and figure 7 shows the cloud chain after the attack.

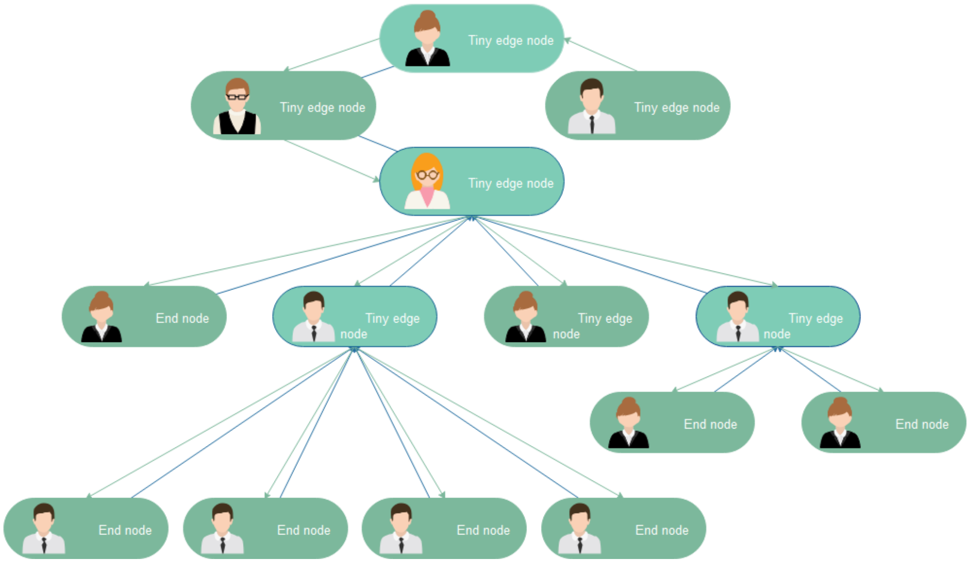


Figure 6. cloud chain before attack

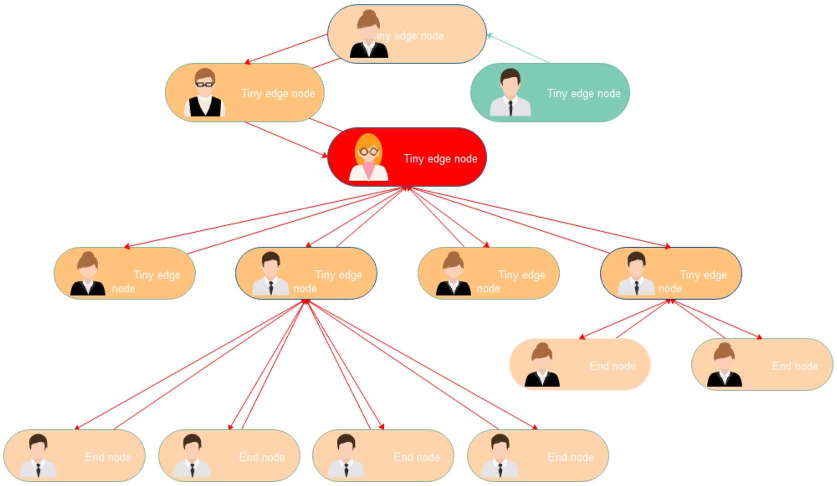


Figure 7. cloud chain after attack

V. RELATED WORK

Ordinary survey papers are limited to the conclusion of research papers, but this paper tries to break the regulation, using prediction method to organize all the pages, which is helpful for researchers to explore the detail of these. This will attract numerous researchers working on it.

In “Service-Oriented Cloud Computing Architecture” [32] , the authors introduce us to the cloud computing system architecture model, which divides the service patterns of cloud computing systems into three categories: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).At the same time, they also introduced the specific structure of the three models, and then analyzed their applications. In “A survey on security issues in service delivery models of cloud computing”[38], the author also comprehensively discusses the security challenges faced by the three service delivery models. In the SaaS model, the author discusses data security, network security, data integrity, data leakage and other challenges in depth. In the end, the author lists the solutions to the current challenges.

In “The emergence of edge computing” [12], “The case for VM-based cloudlets in mobile computing” [16], “A survey on mobile edge computing” [17], the “Edge Computing VS Fog Computing” [20], “A Survey on the Edge Computing for the Internet of Things” [22], “Fog computing and its role in the internet of things” [23] and “Fog-based computing and storage offloading for data synchronization in IoT” [24], these papers draw us a clear map of the EC ecosystem, including three basic models – Fog Computing, Cloudlets and Mobile Edge Computing; the advantages of EC; and some important applications, such as IoT, VR and AR, etc. While in “Edge Computing: Vision and Challenges” [21], “Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges” [25], “Security and trust issues in Fog computing: A survey” [26], “Mobile Edge Computing: Opportunities, solutions, and challenges” [27], “Cloudlet deployment in local wireless networks: Motivation, architectures, applications, and open challenges” [30], “Fog of Everything: Energy-Efficient Networked Computing Architectures, Research Challenges, and a Case Study” [31] these papers provide us the open challenges in the EC paradigms.

Based on the above mentioned, our paper makes contributions through expending the related work by making a conclusion of all the concepts of EC and CC, apart from that, we conclude the challenges of EC and CC, besides, we also make a brief comparison of the challenges between CC and EC. By doing that, we hold a strong belief that the evolution should keep on – from CC to EC, and from EC to a more complex but convenient and safe paradigm. Hence, we further propose our own definition of All-in-Cloud (AiC) and our future expectations of it. Besides, we also dig out some potential challenges of AiC to the researchers, including privacy leakages, protocols of standardization, cost of deployment and “Chain Reaction”.

VI. CONCLUSION

This paper focuses on the All-in-Cloud period and tries to give possible challenges of data privacy and security and future expectations of AiC. Based on the fact that the cloud is replacing traditional data centers, at the same time, we use a different view to construct the knowledge of the cloud, using time dimension to predict the future of the cloud. This paper also compares each period of cloud and essential differences of old version of cloud to propose the AiC structure, which helps form the future work of AiC. With reasonable structure of AiC, we point out essential challenges of AiC, which helps more researchers understand the basic ideas of the cloud future. This paper not only forms the basic understanding of the cloud technology, but also extends the cloud into future expectations. We strongly believe that in AiC period, the revolution of the cloud will bring complete changes to the world, and thus change the way we live.

VII. REFERENCE

[1]. What is cloud computing. Available: https://www.rackspace.com/cloud/cloud-computing.

[2]. Definition: Edge computing. Available: https://searchdatacenter.techtarget.com/definition/edge-computing

[3]. Alibaba Cloud Computing summit meeting, Available: https://yq.aliyun.com/articles/694638?spm=a2c4e.11153940.0.0.1e662e3eBfTJfx, 2019.03, Beijing

[4]. AWS: Netflix case study, Available: https://aws.amazon.com/cn/solutions/case-studies/netflix/

[5]. AWS Public Sector Blog Team, Going "All-In" on AWS: Lessons Learned from Cloud Pioneers,2016, Available: https://aws.amazon.com/cn/blogs/publicsector/going-all-in-on-aws-lessons-learned-from-cloud-pioneers/

[6]. Apple, iCloud: The best place for all your photos, files, and more, Available: https://www.apple.com/icloud/

[7]. IDC FutureScape: Multiplied Innovation Takes Off, powered by AI, Distributed Public Cloud, Microservices, Developer Population Explosion, Greater Specialization and Verticalization, and Scaling Trust. 30.Oct.2018, Available: https://www.idc.com/getdoc.jsp?containerId=prUS44417618#35a1d2a07b96

[8]. Business insider, "EDGE COMPUTING IN THE IoT: Forecasts, key benefits, and top industries adopting an analytics model that improves processing and cuts costs", 2016, Available: https://www.businessinsider.com/edge-computing-in-the-iot-forecasts-key-benefits-and-top-industries-adopting-an-analytics-model-that-improves-processing-and-cuts-costs-2016-7

[9]. The Guardian, "Online all the time – average British household owns 7.4 internet devices", 2015, Available: https://www.theguardian.com/technology/2015/apr/09/online-all-the-time-average-british-household-owns-74-internet-devices

[10]. Prevent Disaster in the Data Center, Available: https://cioupdate.com/prevent-disaster-in-the-data-center/

[11].IDC 2019: Cloud IT Infrastructure Revenues Decline in Q2 2019 Amid a Slow Down in Overall Spending, According to IDC, Available: https://www.idc.com/getdoc.jsp?containerId=prUS45552219

[12]. Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1),30–39.

[13].Khan, Wazir & Ahmed, Ejaz & Hakak, Saqib & Yaqoob, Ibrar & Ahmed, Arif. (2019). Edge computing: A survey. Future Generation Computer Systems. 97. 10.1016/j.future.2019.02.050.

[14]. Cisco fog computing solutions: Unleash the power of the internet of things, available at: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/ computing-solutions.pdf, 2015 (Accessed on 23 July 2018).

[15]. Bao, W., Yuan, D., Yang, Z., Wang, S., Li, W., Zhou, B. B., & Zomaya, A. Y. (2017). Follow Me Fog: Toward Seamless Handover Timing Schemes in a Fog Computing Environment. IEEE Communications Magazine, 55(11), 72–78.

[16]. Satyanarayanan, M., Bahl, P., Cáceres, R., & Davies, N. (2009). The case for VM-based cloudlets in mobile computing. IEEE Pervasive Computing, 8(4), 14–23.

[17]. A. Ahmed, E. Ahmed, A survey on mobile edge computing, in: Proceedings of 10th International Conference on Intelligent Systems and Control, ISCO'16, India, 2016.

[18]. Available: https://www.xianjichina.com/news/details_150922.html. (Accessed on 18 Oct 2019)

[19]. Zhang, P. Y., Zhou, M. C., & Fortino, G. (2018). Security and trust issues in Fog computing: A survey. Future Generation Computer Systems, 88, 16–27.

[20]. Edge Computing VS Fog Computing, Available: https://blog.ipswitch.com/edge-computing-vs-fog-computing (Accessed on 20 Oct 2019)

[21]. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and Challenges. IEEE Internet of Things Journal, 3(5), 637–646.

[22]. Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2017, November 28). A Survey on the Edge Computing for the Internet of Things. IEEE Access. Institute of Electrical and Electronics Engineers Inc.

[23]. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In MCC'12 - Proceedings of the 1st ACM Mobile Cloud Computing Workshop (pp. 13–15).

[24]. Wang, T., Zhou, J., Liu, A., Bhuiyan, M. Z. A., Wang, G., & Jia, W. (2019). Fog-based computing and storage offloading for data synchronization in IoT. IEEE Internet of Things Journal, 6(3), 4272–4282.

[25]. 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.

[26]. Zhang, P. Y., Zhou, M. C., & Fortino, G. (2018). Security and trust issues in Fog computing: A survey. Future Generation Computer Systems, 88, 16–27.

[27]. Ahmed, E., & Rehmani, M. H. (2017, May 1). Mobile Edge Computing: Opportunities, solutions, and challenges. Future Generation Computer Systems, 70, 59–63.

[28]. Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., & Hayajneh, T. (2018, July 19). Security vulnerabilities in bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks. MDPI AG.

[29] Edge Computing VS Fog Computing, Available: https://blog.ipswitch.com/edge-computing-vs-fog-computing (Accessed on 20 Oct 2019)

[30] Shaukat, U., Ahmed, E., Anwar, Z., & Xia, F. (2016, February 1). Cloudlet deployment in local wireless networks: Motivation, architectures, applications, and open challenges. Journal of Network and Computer Applications. Academic Press.

[31] Baccarelli, E., Naranjo, P. G. V., Scarpiniti, M., Shojafar, M., & Abawajy, J. H. (2017). Fog of Everything: Energy-Efficient Networked Computing Architectures, Research Challenges, and a Case Study. IEEE Access, 5, 9882–9910.

[32]. Tsai W, Sun X, Balasooriya J. Service-Oriented Cloud Computing Architecture. ITNG2010 - 7th International Conference on Information Technology: New Generations (2010) pp. 684-689

[33] Effective Privacy Preservation in Third-Party Cloud Storage Auditing

[34] Cao, K., & Jain, A. K. (2015). Learning fingerprint reconstruction: From minutiae to image. IEEE

Transactions on Information Forensics and Security, 10(1),

104–117.

[35] Fielding, R. T., & Reschke, J. F. (2014). Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing. Online.

[36] What is a TCP/IP Available: https://www.iplocation.net/tcp-ip [Accessed

on 20 Oct 2019]

[37] Yongli. Z, Wei. W, Yajie. Li, Carlos. C.M, Massimo. T, Jie. Z,” Edge Computing and Networking: A Surveyon Infrastructures and Applications”, August 9, 2019

[38] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications,2011,34(1):1 11