Scientific Research Publishing

Journal of Computer and Communications, 2017, 5, 80-95
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Quick Survey on Cloud Computing and Associated Security, Mobility and IoT Issues

Michael Perez, Sanjeev Kumar

Department of Electrical and Computer Engineering, University of Texas-RGV, Edinburg, TX, USA
Email: sjkumar1@ieee.org

How to cite this paper: Perez, M. and Kumar, S. (2017) A Quick Survey on Cloud Computing and Associated Security, Mobility and IoT Issues. *Journal of Computer and Communications*, **5**, 80-95.
https://doi.org/10.4236/jcc.2017.512009

Received: June 22, 2017
Accepted: October 28, 2017
Published: October 31, 2017

Copyright © 2017 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

This survey paper provides a general overview on Cloud Computing. The topics that are discussed include characteristics, deployment and service models as well drawbacks. Major aspects of Cloud Computing are explained to give the reader a clearer understanding on the complexity of the platform. Following this, several security issues and countermeasures are also discussed to show the major issues and obstacles that Cloud Computing faces as it is being implemented further. The major part of countermeasures focuses on Intrusion Detection Systems. Moving towards Mobile Cloud Computing and Internet of Things, this survey paper gives a general explanation on the applications and potential that comes with the integration of Cloud Computing with any device that has Internet connectivity as well as the challenges that are before it.

Keywords

Cloud Computing, Cloud Service Models, Platform, Security, Mobility, Internet of Things (IoT)

1. Introduction

Cloud computing is a model that is completely based on the Internet and remote servers to utilize large amounts of data, software, and applications. It is a promising new platform for services to be provided on the Internet. These include storage, applications, and hardware services that clients can utilize as an on-demand basis. The listed services are provided without the clients having to own the particular service or application. As for hardware services, clients do not have to have them installed locally. They are usually paid for by clients "per use" basis, which results in overall cost reductions. Along with reduced costs, major companies such as Google and Amazon utilize the features and benefits of cloud

computing such as low investment cost, easy to manage, and flexibility to provide their services [1]. The purpose of this survey paper is to give the reader a much clearer understanding of the fundamentals of cloud computing ranging from a general overview of cloud computing to the security issues and vulnerabilities that are involved with the platform.

The topics presented in this paper can be divided into four major categories. This includes a general Cloud Computing overview, Cloud Computing security, Mobile Cloud Computing, and Internet of Things. For the cloud computing overview, the reader will find detailed explanations for each individual aspect of cloud computing to get a clearer understanding on the platform ranging from its architecture to each service model. The cloud computing security section will provide an overview of a variety of different security threats and vulnerabilities that cloud computing faces. Mobile Cloud Computing and Internet of Things both act as extensions to the general overview of Cloud Computing with subtopics including Cloud Computing limitations, new applications, and the future outlook, as Cloud Computing is further integrated with mobile devices.

2. Cloud Computing General Overview

There are various levels of Cloud Computing that need to be taken into consideration when trying to understand the platform. Like most forms of technology it has it's own set of benefits and drawbacks, which will be discussed shortly, but also has defining characteristics that set it apart from other forms of technology. Other levels of cloud computing include the various service and deployment models. Each of these models allows for versatility in order to satisfy a specific set of needs for different customer bases. On a higher level the cloud architecture can be used to describe each component of cloud computing ranging from the physical servers and networks, the middleware, and even to individual application function that are more commonly associated by clients for cloud computing. **Figure 1** shows a general overview of each architectural layer of cloud computing.

2.1. Cloud Computing Architecture

It is suggested that cloud computing can be divided into three levels with each layer representing a key part of cloud computing. The application layer contains the data and various applications used by clients such as web interfaces, programming interfaces for application development, and the main engines for cloud applications known as the application core. The virtualization layer backs up applications by providing them with the necessary resources and demands. Database access and server functionality is found at this layer as well as connectivity components such as Internet Protocol and Domain Name System (DNS). Here also, the virtualization of the physical infrastructure is provided where anything related to virtual machines is defined and controlled from the virtual

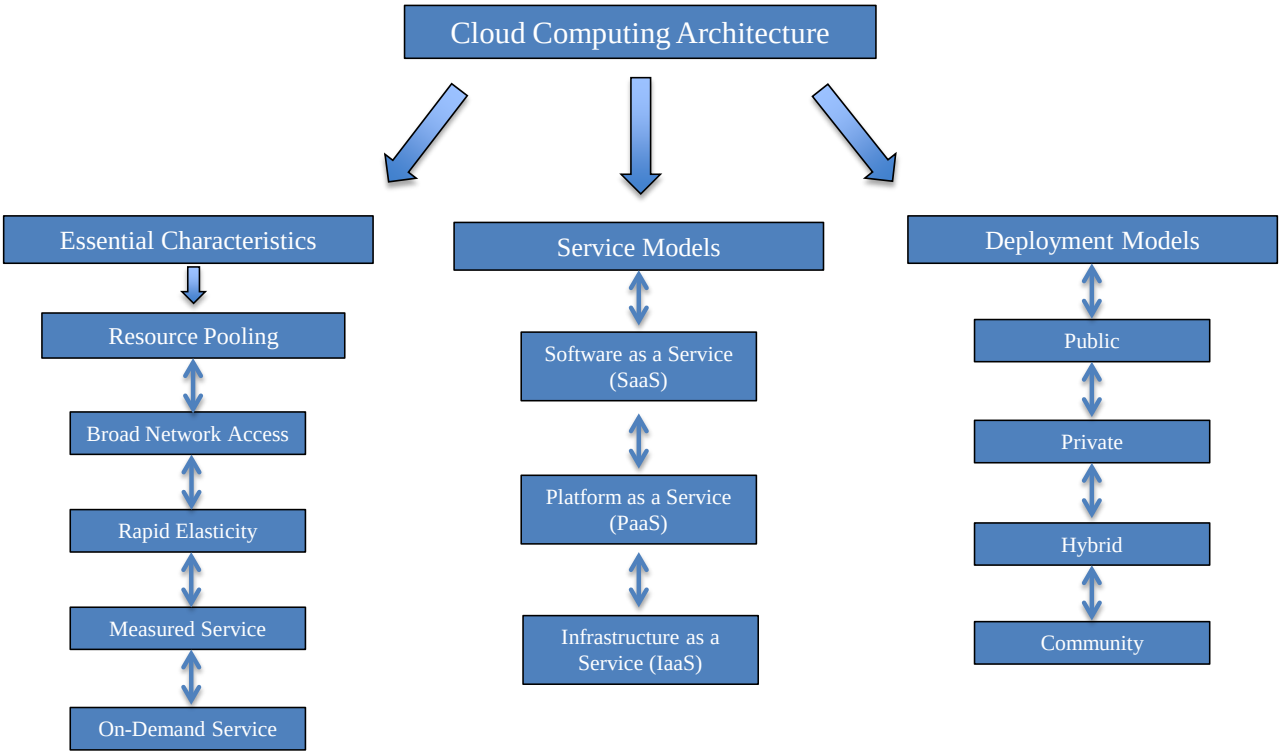

Figure 1. Cloud computing architecture and general overview.

components. The physical layer is the hardware and resources that the two layers above utilize to perform their required tasks. Hardware includes individual servers, switchers, and routers. The facilities that house the hardware is also a part of this layer along with the power systems related to maintaining proper operation of the physical components in house. This includes heating, ventilation, air conditioning, and emergency power [2].

2.2. Cloud Computing Benefits

The adoption of cloud computing has allowed for many companies to experience several benefits from it's implementation. Reduction of costs from different payment schemes such as a onetime payment or pay-as-you-use instead of an extensive purchase of a large number of computers and related hardware has been a major benefit. Also the combination of needs from a customer base reduces the overall cost and with the higher computer utilization from cloud computing services, this makes it an enticing option for major companies. Another benefit offered is the reduced deployment times. With cloud computing, whole systems can become fully functional in a fraction of the time traditional methods would have. Examples include virtual web servers that can be brought online in the cloud and the launching of products or services [1] [3]. Different aspects of services also benefit from cloud computing including introducing new services, scalability, and easy access. The cloud allows information to be easily accessible anywhere with proper access. For scalability, the cloud can scale services and provide new ones easily with the demands of customers. Along

with this, backup and recovery is another key benefit of cloud computing, which allows easier storage than physical media [1].

2.3. Cloud Computing Drawbacks

Like all other forms of technology with all the benefits that cloud computing offers there are some drawbacks. Security issues are the main drawback to cloud computing as sensitive data is usually handed over to third party cloud servers, which could lead to trust issues within organizations of who they work with. The amount of data used in cloud computing also makes it vulnerable to attacks, which requires constant monitoring. Also technical issues such as server downtimes and even data losses can hinder job completions from organizations. Application inflexibility can also be considered a drawback to cloud computing because of the lack of support for different formats [1].

2.4. Cloud Computing Characteristics

With Cloud Computing being so complex there are several basic characteristics that define the technology that is universally understood as the foundation for the platform. These characteristics allow the services of Cloud Computing to be provided which include elasticity, on demand self-service, multi-tenancy, and shared resource pooling to name a few [1] [3] [4].

Elasticity allows cloud computing to scale either up or down quickly in order to make a user think that there are unlimited resources available at all times. Multi-tenancy allows the same infrastructure to be shared by different businesses. Each one would have its own responsibilities of its own respective layer while sharing the same infrastructure provider and same data center. Shared resource pooling allows the provider to combine computing resources to serve different customers, and assign and reassign physical and virtual resources as customer demand changes. This allows more flexibility to the infrastructure providers for resource management and costs. Broad network access is another key characteristic of cloud computing. Since the platform is Internet based, the only thing required for any Internet ready device to access cloud mechanisms, services, and resources is an Internet connection [1] [3] [4].

2.5. Cloud Computing Deployment Models

The type of model cloud computing can be classified as depends on location and organization. Public clouds are considered the standard cloud model. Multiple users access the cloud resources and services on the same public infrastructure. Each user is charged by the amount of time accessing the resources that they need. Drawbacks to this model include the fact that it is prone to attacks and have various security issues that will be discussed in later sections.

Private clouds contain an individual in a protected cloud environment which only the single user can utilize the cloud services. On an organizational level, the cloud is only assessable within the same company and it is also managed inter-

nally. Benefits include security and easy maintenance however; the privatization of this cloud can result in high costs. A community cloud is implemented as an access between several organizations and belongs to the same community. Privacy requirements, policies, and security concerns are all shared. Infrastructure locations can vary such as the same company hosted by a third-party. Hybrid clouds combined private and public clouds or multiple clouds of the same type under a standard protocol. Companies can utilize aspects of which types of clouds are present in the hybrid cloud to allocate where to perform certain tasks that can improve productivity [1] [5].

2.6. Cloud Computing Service Models

There are three service models used to describe cloud services. These include Software as a Service, Platform as a Service, and Infrastructure as a Service. Software as a Service (SaaS) allows clients to access cloud applications without having to install the application on their own computer. The service provider maintains the cloud-computing infrastructure, and control from a user's standpoint is only at the application settings [6]. The advantages of this model include reduction of software licensing costs, security, and it allows multiple clients to use the same application at the same time [7]. Platform as a Service (PaaS) is somewhat opposite of the previous model where now clients can create and deploy their own applications to the cloud. These applications are developed by programming and configuration tools and are mainly used by developers, testers or administrators [6]. This platform allows individuals to develop applications without the need to have the proper environment installed locally. Control over the application's configuration is in the client's hands while the actual cloud infrastructure is not since they are renting the virtual servers for development and testing. Advantages of Platform as a Service include increased flexibility for developers allowing them to create new platforms on demand to meet newer requirements along with security benefits of the service for data, which include backup and recovery [7]. Infrastructure as a Service (IaaS) the client now has access to the actual infrastructure of the cloud service provider. They can use the virtual hardware to use development tools to build applications on the given infrastructure. Clients include higher level IT personnel including system administrators and developers [6]. Advantages of Infrastructure as a Service include fluctuation of the infrastructure on demand and reduction of costs from hardware and human resources as well as from the ability to have many users use single hardware [7].

3. Cloud Computing Security

Each level of Cloud Computing can have the potential for security risks that need to be taken into consideration. The number one concern with the amount of data being processed and stored in clouds is data security and privacy. In most cases users and clients do not know this information, as this aspect of Cloud Computing is essential but out of their hands. This concern of Cloud Computing

will be discussed in further detail. Looking at various security threat examples and countermeasures pertaining to topic discussed previously such as Cloud Computing service models and characteristics can give a good overview on the obstacles that Cloud Computing faces as it is further implemented and more widely used.

3.1. Cloud Computing CIA Triad

The CIA Triad model stands for Confidentiality, Integrity and Availability for securing systems and plays a key role in maintaining proper security for cloud computing. With the amount of data being exchanged on the platform each part of the triad must be kept in check. Confidentiality prevents the access of data by unauthorized party and in essence main role is to keep data private. There are several parts of cloud computing that are related to this part of the CIA Triad. Encryption, covert channel, and traffic analysis are just a few examples of what is associated with confidentiality in cloud computing. Integrity maintains consistent and unaltered information being used on the cloud. This means that there is no unauthorized modification of data present. Availability in cloud computing means that the resources and data are reliable and can be accessed at any time as user needs [8] [9].

3.2. CIA Triad General Security Threat Examples

General security threats also apply to cloud computing such as eavesdropping, fraud, theft, and external attacks. Each of these affect the CIA Triad for cloud computing. Eavesdropping allows the unauthorized gathering of information, fraud can be either data manipulation or falsification, and external attacks can result in lack of availability for cloud computing services. There are several techniques used to compromise the CIA Triad for cloud computing. Reconnaissance can involve various methods of collection methods and social engineering to gather information to be granted unauthorized cloud access. These can include physical break-ins to get to specific machines to access information, dumpster diving to retrieve discarded information which can sometimes still be valid, and social engineering to manipulate individuals into giving out secret information such as passwords. Denial of Service is the main culprit for affecting the availability of cloud computing in the CIA Triad. Resources such as CPU, Network, and Memory are the main targets to bring down access to cloud related services. General methods implemented can be buffer overflows and packet flooding. Other general methods used to violate the CIA Triad include account cracking and malicious software. Account cracking from brute force password attacks can lead to unauthorized access to accounts and thus can result in data manipulation and data being stolen. Malicious software such as viruses, spyware, and worms can all in their own way affect each part of the CIA Triad [9].

3.3. Cloud Computing Threats and Countermeasures

With the amount of sensitive applications and data taking part in cloud compu-

ting there are various aspects of the technology where specific security issues can take place. Security threats in the cloud computing environment have their own exploits for taking advantage of different vulnerabilities. In virtualization, with the amount of operating systems running on single hardware, it is possible to loose track of all the machines present. This can result in a new machine running malicious code to either gain control of the entire system or bring the system down. Rootkits can be installed to infect machines to hide key components from being identified by different security tools and programs. Countermeasures for this type of attack revolve around authenticity checks for messages from the client machines. A comparison of an original image file to upcoming service request via hash values is one specific method.

The software interfaces that clients use for cloud computing also have their own set of risks. The control over several virtual machines and systems in combination with potential insecure interfaces and application program interfaces can lead to unauthorized access, reusable passwords, and limited logging to name a few. Countermeasures can include strong authentication methods and encrypted transmissions. The storage of data by third party data center can result in data breaches that leak information and cause data corruption. In particular, by renting a server from other service providers for reduction of costs and flexibility, cloud providers run the risk for malicious insiders to steal the valuable data on the service provider servers. There are multiple security threats that can result in data breaches such as identify theft, malware, SQL injection, and phishing. Data breach aftermaths can result in cloud service providers to close because of the financial and legal issues that arise with customer data loss and corruption. Countermeasures include filter techniques for user inputs, active content filtering for SQL attacks, and web application vulnerability detection.

Related to the data breach risks stated previously, since data in cloud computing can be stored anywhere in the world this can lead to access problems for clients. This makes any type of localized attacks at the storage areas completely out of the customer's control. For a customer and provider, knowing who is managing their data and what are their privileges is part of the preventative maintenance process for making sure their data is secure. With storage locations being unknown, identity management and authentication is key. Brute force attacks can decrypt passwords and lead to unauthorized access. On a related note, with storage facilities being all over the world there are privacy concerns that are associated in the cloud-computing environment. Different countries may have different privacy regulations with their own restrictions and guidelines on data security. This can lead to data being prone to man-in-the-middle attacks and other eavesdropping techniques. The countermeasures to protect data because of data location and the privacy issues include high-level password authentications and data access policies, sniffing detection platforms, and separating endpoint and server security processes [10].

3.4. Security Threats to Cloud Computing Characteristics

Looking at the characteristics of cloud computing that were discussed in a previous section, here we can find and describe security risks to the cloud service environment. The elasticity nature of cloud computing makes security breaches possible even though safety measures are in place such as data encryption. For multi-tenancy, the service placement engine, which overlooks the lists of available resources for the cloud resource pool, must have several security requirements. These are needed to avoid the placement of multiple cloud services on the same hardware resource, which can create data vulnerabilities. With shared resource pooling comes a certain distribution and multi-user environment. Here risks are always present because of the lack of control users have in this type of environment. Referring back to the previous section on specific CIA threats with the issues of control over data and applications, since customers have to trust the service provider with sensitive data without knowing exactly where the services or applications are located in general, the data itself is vulnerable in each area of the CIA triad. Adding on to characteristics, there is also a lack of standard at each cloud tier. High flexibility in a cloud computing environment can make users become dependent on only one service provider which can make them even more vulnerable from the lack of diversity [11].

3.5. Security Threats to Cloud Computing Service Models

Each service model has its own set of unique vulnerabilities based on its structure. This comes from the differences in what is managed by users and the cloud service providers for each service model. Software-as-a-Service (SaaS) specific vulnerabilities include identity management, lack of standards, service secrecy, anywhere access, and general infrastructure security. For identity management the use of third parties creates differences in how they approach restricting system access to authorized users increases vulnerabilities. Also with lack of standards and service secrecy, the fact that the information on where data is stored and the lack of disclosers on how it is secured creates vulnerabilities for users. With this lack of information the service providers do not guarantee the safety of data other than just general formalities saying that the data is secured. With this service model, since access can occur anywhere, individual users and endpoints cannot be guaranteed to be secure. This can create openings for threats to this cloud service model. Now as stated before, there will be issues with data security when running an application on the cloud as the infrastructure security is totally dependent on the service provider.

Platform-as-a-Service model vulnerabilities include attacks that affect availability, API security, platform applications upgrades, and general development security. This service model is susceptible to Denial of Service (DDoS) attacks. With no standards for API security this makes authentication issues arise which can lead to the cloud to be exposed to attacks from other users. The upgrading of platform components and patch updates together can stop possible service down-

time because of this. Overall changes though can lead to compromised data and applications. With this service model providing the development environment tools to customers, the customers do not have a guarantee that they are secure.

Infrastructure-as-a-Service (IaaS) model vulnerabilities include enforcement of Service Level Agreement, virtualization, and security of virtual machines. The enforcement of service level agreements has to be done by both the cloud service provider and customers when necessary. The lack of enforcement and monitoring of quality of services can create security issues. For virtualization, changes to virtual machines in general can create security threats and the lack of a controlling system to monitor virtual machines and the communications that take place also creates a high-risk environment. The security of virtual machines in particular the communication and mobility must be secure to prevent cloud servers from being susceptible to DDoS related attacks. Overall, for the three service models they each share vulnerabilities that relate to the CIA triad such as each one can be susceptible to DDoS attacks, which affect availability, or the assurance of information, which affects confidentiality, and maintaining data integrity in general [11].

3.6. Intrusion Detection Systems

The previously mentioned cloud computing threats can be categorized into two areas, they are insider attacks which include cloud users doing unauthorized tasks, and outsider attacks such as DDoS. Preventing these attacks is a challenge for Intrusion Detection Systems (IDS) [12]. "The definition for Intrusion Detection Systems is the process of monitoring events occurring in a computer system or network and analyzing them to look for intrusions" [12]. The system itself can be both hardware and software. However there are some limitations to existing IDS that make it a challenge to work within the cloud-computing environment. They do not have autonomic self-adaptation, lack scalability, and are not deterministic. Thus new cloud based IDS are needed [12].

Looking at the detection techniques used by IDS they are categorized by signature based, anomaly based, and hybrid based detection. Signature based detection compares current information on a network to a pre-established database of signatures that is used to determine if current information corresponds to an attack. Pattern recognition techniques are used by this method in the decision making process of whether or not current traffic matches to a known signature. Benefits to this type of detection method is that it has high accuracy and is flexible as new signatures can be added to the database to keep the system up to date. One major drawback though is the fact that it relies on a current database. If an unknown new attack would occur, the system would have no way of recognizing it. Anomaly-based detection actively tries to find suspicious activity on a network or system. Preload profiles are used with current user activities to detect any possible intrusions. Profiles are created within a given timeframe known as a training period, which the regular activities of users and overall network usage

are considered. This gives the IDS time to identify habits within a network over a certain period of time such as CPU usage, file access times, and incorrect logins. The benefit that this type of detection has over signature-based is that it can detect unknown attacks by comparing current network and system activities to the profiles that it has created to determine that an attack is taking place. Hybrid detection is the combination of signature-based and anomaly-based detection using both methods as one IDS [12].

3.7. Cloud Computing Intrusion Detection Systems

The types of cloud-computing IDS are Network based, Host based, Distributed, and Hypervisor-based. Network based IDS can use both signature and anomaly based techniques to identify potential malicious activities. After it scans the traffic for a network, it uses the IP and transport layer headers of each packet in its detection. This type of system however, cannot analyze encrypted traffic and intrusions in a virtual network by a virtual machine monitor which creates and runs virtual machines.

Host based IDS instead of collecting information from the entire network it collects and analyzes information from a specific host machine to detect any possible intrusions. Information that is used includes network events, system calls, and file usage to name few. Any modification in the host kernel, host file system, or overall behavior of the program that seems to be unusual is reported as an attack. In cloud computing, Host based IDS can be deployed on the hypervisor (creates and runs virtual machines) or host. Here it can use system logs, user logins, and policies to detect any potential threat within the cloud. Benefits over Network based IDS include the ability to now analyze encrypted traffic, but this type of detection system is vulnerable to DDoS attacks.

Distributed IDS combines many Network based and Host based IDS, which are deployed on a large network. Each individual IDS communicate with a centralized server.

Hypervisor-based IDS is used for virtual machines as it is set up at the hypervisor layer. This system monitors communication at different levels such as communication between virtual machine and hypervisor to detect any type of anomalies [12].

4. Mobile Cloud Computing

Mobile Cloud Computing has been made prominent with the dramatic rise of mobile devices being connected to the Internet. Mobile Cloud Computing is defined as a system in which both the data processing and data storage are performed outside the mobile environment [13]. With applications needing constant access to the Internet the services provided by Mobile Cloud Computing can offer convenience and ease of use. Applications now have a larger scope with computations and data storage being used in the cloud instead of being all directly on the mobile device [13]. Looking first at the architecture of Mobile

Cloud Computing can allow for a better understanding of the platform and the differences between itself and regular Cloud Computing.

4.1. Mobile Cloud Computing Architecture

Mobile cloud computing services have some differences than the cloud services as regular cloud computing with Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). This is due to these classifications being based on virtualization [14]. With the increasing number of mobile clients in cloud computing using mobile applications that are linked to servers operating in the cloud, breaking down mobile cloud computing architecture into its components can help with understanding how mobile devices and clients work with cloud computing. These components are mobile clients, middleware, and cloud services. Each mobile client connects to the cloud, which is managed by service providers' thorough middleware. The middleware component pushes updates to services via hypertext transfer protocol [15].

For mobile cloud service models, they are classified based on the roles of computational entities within a service framework. Specific models are titled Mobile as a Service Consumer (MaaSC), Mobile as a Service Provider (MaaSP), and Mobile as a Service Broker (MaaSB). The most popular model for mobile cloud computing is MaaSC. Mobile devices using this model can achieve higher performance and have a broader range of application capabilities by outsourcing computation and storage to the cloud. MaaSP is the opposite of MaaSC where now each client has the capability of the service provider. Services provided here are based on sensing and processing capabilities of the connecting mobile devices with application data ranging from GPS, camera, and other device related data. Other local devices receive this data in order to improve performance and accuracy of various applications. MaaSB is used when mobile devices are limited in their capabilities. This model allows an extension to sensor networks where a mobile device can be used as a gateway to provide network services via Bluetooth, WiFi, and cell phone provider network in order to communicate and send data to cloud resources. Mobile devices can also act as a security layer to sensor networks under this service model [14]. **Figure 2** shows an overview of each mobile cloud service model.

4.2. Mobile Cloud Challenges

Similar to regular Cloud Computing, the challenges with Mobile Cloud Computing revolve around security and resources especially with the mobile devices themselves. Each mobile device can have limited battery and computational power in comparison to desktop and laptop computers, which is a major factor to take into consideration when using applications on the cloud. Also with varying signals and network problems that mobile device carriers can have may lead to inefficient operation. This can lead to the lack of Internet connectivity which means cloud operations will not be fully functional. For security, the risks are

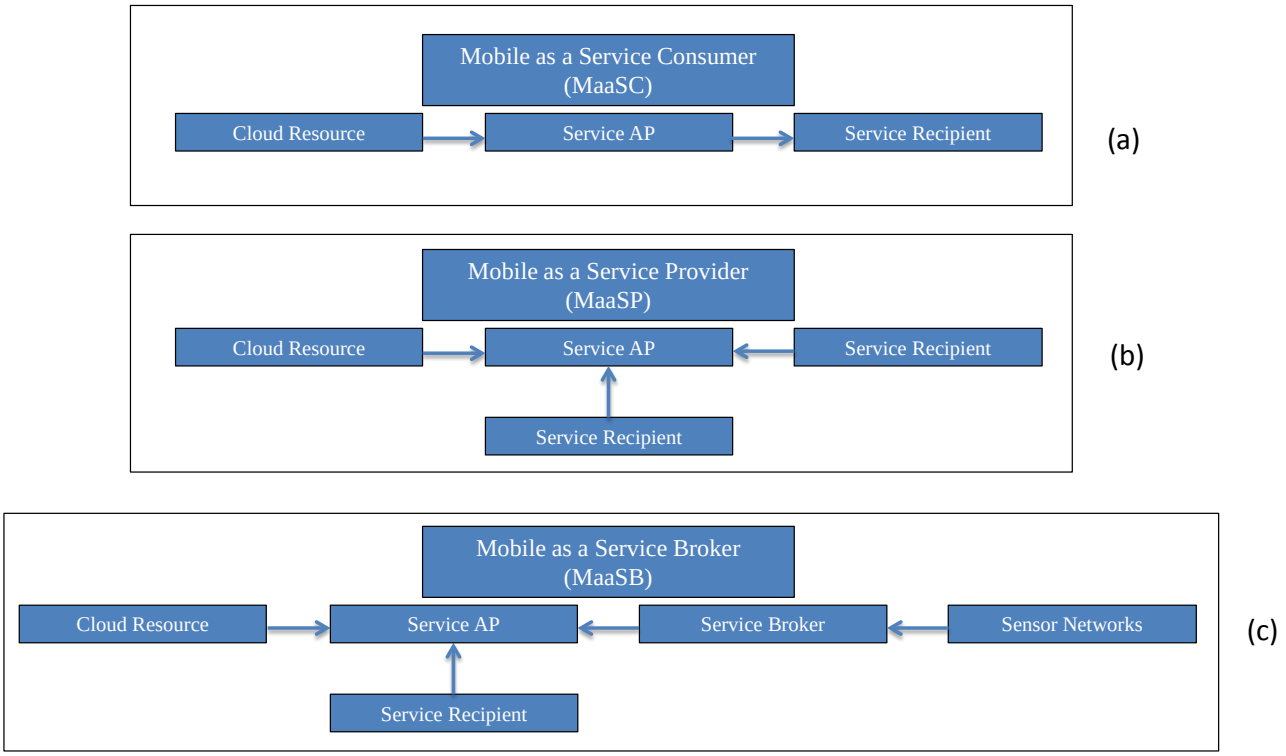

Figure 2. Mobile cloud computing service models: (a) Mobile as a service consumer model; (b) Mobile as a service provider; (c) Mobile as a service broker.

similar to traditional devices that connect to the Internet as mobile devices are at risk for malicious attacks as well as the general cloud security [13], which was discussed earlier in the paper.

4.3. Mobile Cloud Applications

Current applications that are being used as a result of the increased popularity of mobile devices are email, banking, healthcare, and gaming to name a few. Email acts as the main application of the Mobile Cloud as emails are stored on a remote server and are accessed and updated regularly by mobile devices. Banking and commerce in general, is utilizing the Mobile Cloud for performing different transactions such as Mobile Banking and shopping. For healthcare the Mobile Cloud is used to provide better overall service and treatment for patients such as ease of access of patient health records. On the entertainment side, Mobile Gaming has taken advantage of using the Mobile Cloud for computing resources to allow users to play advanced type of games on their mobile devices [13].

The list of mobile cloud applications described in [14] includes computation, storage, security and privacy, and context awareness. One obstacle faced by mobile cloud computation is that dividing tasks between a local mobile device and the cloud can be inefficient leading to high energy consumption, CPU usage, and network delays. Various services mitigate these inefficiencies by offering runtime environments to make mobile applications run seamlessly between local devices and the cloud servers. Other services use code to maximize energy consumption

as well as offloading tasks to the cloud is made efficient by having this process to be automatic. For mobile cloud storage, automatic synchronization is a preferred feature to send data to storage services. Examples of storage services include Dropbox and Google Drive. Each mobile device has a limited amount of storage capacity and sensitive data used in automatic synchronization such as history, contacts, and preferences has to be kept in a secure and reliable space [14].

5. Internet of Things (IoT)

With the concept of Internet of Things (IoT) now a reality, the amount of devices connected to the Internet has grown exponentially. The combination of cloud computing, sensors, and actuators creates a network never seen before. These smart devices can range from practically anything including wearables, security solutions, healthcare, smart electric meters, smart appliances, and power grids to name a few [16]. The incorporation of these devices with cloud computing has increased performance potential and they also have many challenges.

5.1. Internet of Things and Cloud Computing

Cloud IoT is the name given for the combination of Internet of Things and Cloud Computing. Cloud Computing has most of the issues that Internet of Things has solved with nearly unlimited capabilities in processing power and storage. Now Internet of Things can also benefit Cloud Computing by extending its scope and bring new types of services. Looking at specifics, Internet of Things produces a large amount of data from the information it gathers and Cloud Computing is the most cost effective and convenient way to handle the amount of data produced by Internet of Things. For processing power, each Internet of Things device has limited processing power and resources. Usually data is transferred to more powerful capable devices for processing. Cloud Computing can offset this drawback of Internet of Things and create higher levels of complexity with these devices. Looking at connectivity, each device that is part of Internet of Things has to be IP-enabled and the costs for support can be rather high. Cloud Computing offers a much more cost-effective solution and these devices can be managed and monitored in real-time from applications on the cloud. Overall the addition of Cloud Computing to Internet of Things can solve the issues of scalability, reliability, and security [17].

5.2. Cloud IoT Applications

The area of healthcare can benefit greatly from Cloud IoT as it creates a solution to managing healthcare sensor data efficiently. Mobile devices that are tailored for healthcare can be made more secure and available as with regular Internet of Things devices they generate a large amount of data that has to be managed and processed. With the introduction of Cloud Computing, these devices can allow for innovation in this industry, and create cost effective, efficient, and high quality services [17].

Smart Home applications can range from managing energy consumption, lighting, and air conditioning. Each relies on a sensor network, which can produce a large amount of data. The rise of home automation and Internet-enabled devices in a household create an opportunity for an integration of a cloud to manage these devices. The cloud must provide internal network connections, intelligent remote control, and automation. Another home related application is video surveillance. Using the cloud can mitigate any potential storage constraints that may arise with the amount of data gathered in surveillance. Cloud based solutions can be used to store and mange content from surveillance feeds and deliver it to authorized user devices via the Internet [17].

Smart Energy can utilize Cloud IoT to provide intelligent management of energy systems such as energy distribution and energy consumption. For distribution, electricity can be better managed by providing services after analyzing data collected from nodes that have sensing, processing power, and network capabilities. Each node along with the cloud can distribute tasks and the decision-making can be made on the cloud [17].

The automotive industry also can have many benefits with the integration of Cloud Computing and Internet of Things with transportation technologies. These IoT-based vehicular data clouds benefits can include increased road safety, reduced traffic, and vehicle maintenance [17]. "Vehicular Clouds are designed to expand the conventional Clouds in order to increase on-demand the whole Cloud computing, processing, and storage capabilities, by using underutilized facilities of vehicles" [17]. Issues with vehicular clouds include scalability due to the amount of vehicles and number changes. Along with this the various speeds and locations where vehicles travel can cause interruption in communications, which reduce performance, reliability, and quality of service. Security is also an issue due to the lack of an established infrastructure preventing any effective authentication [17].

6. Conclusion

In summary, this survey paper provides a general overview of Cloud Computing and various subtopics related to the technology behind it including mobile, security and IoT. The scope and potential for Cloud Computing can be endless but it has several drawbacks and security risks that need to be addressed in order for it to become more reliable and more accepted. As a new Information Technology model and platform for the consumptions and delivery of services on the Internet, there are many benefits from both a business and personal standpoint. These applications can utilize Cloud Computing to provide better and more efficient services as discussed in the previous sections. Full utilization of Cloud Computing has yet to be realized but as the technology and architecture become more adopted along with possible standardizations that are needed, many devices and applications can have a much larger scope and greater performance potential from Cloud Computing.

Acknowledgements

This work was supported in part by the US National Science Foundation, under Grant# 0421585 and Houston Endowment Chair in Science, Math and Technology Fellowship.

References

[1] Kamboj, S. and Ghumman, N.S. (2016) A Survey on Cloud Computing and Its Types. 2016 3*rd International Conference on Computing for Sustainable Global Development* (*INDIACom*), New Delhi, 2971-2974.

[2] Colman-Meixner, C., Develder, C., Tornatore, M. and Mukherjee, B. (2016) A Survey on Resiliency Techniques in Cloud Computing Infrastructures and Applications. *IEEE Communications Surveys & Tutorials*, **18**, 2244-2281. https://doi.org/10.1109/COMST.2016.2531104

[3] Arinze, B. and Anandarajan, M. (2013) Adapting Cloud Computing Service Models to Subscriber Requirements. 2013 16*th International Symposium on Wireless Personal Multimedia Communications* (*WPMC*), Atlantic City, 1-5.

[4] Savu, L. (2011) Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges. 2011 *International Conference on Computer and Management* (*CAMAN*), Wuhan, 1-4. https://doi.org/10.1109/CAMAN.2011.5778816

[5] Mirobi, G.J. and Arockiam, L. (2015) Service Level Agreement in Cloud Computing: An Overview. 2015 *International Conference on Control, Instrumentation, Communication and Computational Technologies* (*ICCICCT*), Kumaracoil, 753-758. https://doi.org/10.1109/ICCICCT.2015.7475380

[6] Polash, F., Abuhussein, A. and Shiva, S. (2014) A Survey of Cloud Computing Taxonomies: Rationale and Overview. *The* 9*th International Conference for Internet Technology and Secured Transactions* (*ICITST*-2014), London, 459-465. https://doi.org/10.1109/ICITST.2014.7038856

[7] Bokhari, M.U., Shallal, Q.M. and Tamandani, Y.K. (2016) Cloud Computing Service Models: A Comparative Study. 2016 3*rd International Conference on Computing for Sustainable Global Development* (*INDIACom*), New Delhi, 890-895.

[8] Kanday, R. (2012) A Survey on Cloud Computing Security. 2012 *International Conference on Computing Sciences*, Phagwara, 302-311. https://doi.org/10.1109/ICCS.2012.6

[9] Patil Madhubala, R. (2015) Survey on Security Concerns in Cloud Computing. 2015 *International Conference on Green Computing and Internet of Things* (*ICGCIoT*), Noida, 1458-1462. https://doi.org/10.1109/ICGCIoT.2015.7380697

[10] Jouini, M. and Rabai, L.B.A. (2014) Surveying and Analyzing Security Problems in Cloud Computing Environments. 2014 *Tenth International Conference on Computational Intelligence and Security*, Kunming, 689-693. https://doi.org/10.1109/CIS.2014.169

[11] Girma, A., Garuba, M. and Li, J. (2015) Analysis of Security Vulnerabilities of Cloud Computing Environment Service Models and Its Main Characteristics. 12*th International Conference on Information Technology New Generations*, Las Vegas, 206-211. https://doi.org/10.1109/ITNG.2015.39

[12] Chiba, Z., Abghour, N., Moussaid, K., El Omri, A. and Rida, M. (2016) A Survey of Intrusion Detection Systems for Cloud Computing Environment. *International Conference on Engineering & MIS*, Agadir, 1-13. https://doi.org/10.1109/ICEMIS.2016.7745295

[13] Mallya, K.R. and Dhas, C.S.G. (2016) Secure Learning in the Mobile Cloud. *IEEE International Conference on Advances in Computer Applications*, Coimbatore, 125-130. https://doi.org/10.1109/ICACA.2016.7887936

[14] Huang, D., Xing, T. and Wu, H. (2013) Mobile Cloud Computing Service Models: A User-Centric Approach. *IEEE Network*, **27**, 6-11. https://doi.org/10.1109/MNET.2013.6616109

[15] Tuli, A., Hasteer, N., Sharma, M. and Bansal, A. (2013) Exploring Challenges in Mobile Cloud Computing: An Overview. *Confluence* 2013: *The Next Generation Information Technology Summit*, Noida, 496-501. https://doi.org/10.1049/cp.2013.2364

[16] Saha, H.N., Mandal, A. and Sinha, A. (2017) Recent Trends in the Internet of Things. 7*th Annual Computing and Communication Workshop and Conference*, Las Vegas, 1-4. https://doi.org/10.1109/CCWC.2017.7868439

[17] Botta, A., de Donato, W., Persico, V. and Pescapé, A. (2014) On the Integration of Cloud Computing and Internet of Things. *International Conference on Future Internet of Things and Cloud*, Barcelona, 23-30. https://doi.org/10.1109/FiCloud.2014.14