Journal of Theoretical and Applied Information Technology
15th March 2018. Vol.96. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PRESENT CHALLENGES AND FUTURE PROMISES OF CLOUD COMPUTING

YOUSRA ABDUL ALSAHIB S.ALDEEN

Department of Computer Science, College of Science for Women, Baghdad University, Baghdad, Iraq

E-mail: yohrmz_8@yahoo.com; yousraalkaalesi@gmail.com

ABSTRACT

Cloud computing (CC) being an attractive and significant information technology (IT) revolution would certainly bring several innovative benefits and services to humankind. Thus, cloud is emerged as a principal buzz and continues to reform the IT industry. The very notion of cloud made it feasible to isolate huge infrastructure mediation and provided the customer services via redefined software and hardware business models. This helped the end users to purchase commodities at minimal along with taking the complete advantages of essential services. However, absolute privacy protection and preservation in cloud assisted data mining is prerequisite. This paper highlights the main challenges in CC and the future application prospects of the existing IT systems to the cloud.

Keywords: *Cloud Computing, Services, Challenges, Security, Privacy*

1. INTRODUCTION

Cloud computing (CC) has become a very common paradigm delivering services over the Internet. The target of such computing model is to have a better use of different distributed resources and put them together in order to realize higher throughput and be able to solve large-scale computation problems. CC is not a fully new concept for the evolution and operation of Internet applications.

A recent research has been proved there is some considerable confusion regarding CC, the majority of respondents believed that cloud is refers to weather cloud on the sky. The results indicated that 29% respondents associated the term cloud with the weather and only 16% replied that it is a computer network, where users store, access, and share data from internet-connected devices. Despite this concept is because of unawareness, the aware users are actually cloud computing users and remaining are non-users. The survey therefore clearly demonstrates that cloud computing is not just in widespread use, but indeed ubiquitous. However, most people have no idea about cloud computing, when they are using cloud computing in their daily activities and able to avail better services and security, then they realized the importance of this technology[1].

Basically, the idea behind CC is delivering the services over the internet through datacenters, which are equipped with hardware and software servers. These services have long been called SaaS (software as a service) and software and hardware named as cloud. Further the cloud is divided into public and private cloud, the public cloud mean the service is available for general public in the manner of pay-as-you-go and also named as utility computing. The private cloud refers to private business or organizations internal datacenters and not for general public. Thus, the combination of SaaS and utility computing without private cloud is called cloud commuting. The peoples are users and service providers of SaaS or utility computing [2].

Though cloud computing has given considerable opportunities to the IT industries, it also brings numerous particular challenges which should be accurately discussed. This paper presents a survey of cloud computing, highlighting its key concepts, architecture, state-of-the-art models of cloud computing, pros and cons of cloud computing and the most important research challenges which are privacy and security. The goal of this article is to supply a good understanding of cloud computing and identify significant research directions in this area.

The remainder of this paper is organized as follows. In Section 2, I provide the architecture

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of cloud computing. In Section 3, I describe the state-of-the-art of cloud models. The pros and cons of cloud computing are described in Section 4. The research challenges are detailed in Section 5. In Section 6, I discussed this work compare to other studies. Section 7 conclude this paper. Figure 1 shows the literature review process flow.

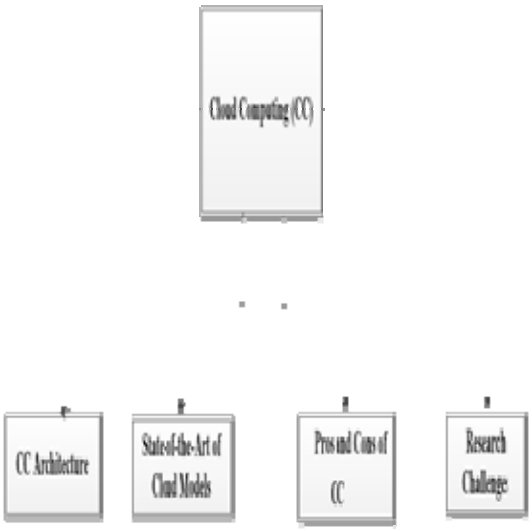

Figure 1 Literature Review Process Flow

1.1. Definition

The analysts have been defined the term cloud computing with subject wise such as different in academics, analyst firms and IT companies. Still the term cloud computing is not clear by means. According to National Institute of Standards and Technology (NIST) the cloud computing is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3]. Pearson et al. had listed [4]. Another author defined the NIST definition and highlighted five important features: broad network access, rapid elasticity, measured service and on-demand self-service[5]. In cloud computing the service models are software as a service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and private cloud, public cloud and community cloud are deployment models.

The important security challenges are considering and focused when using cloud services such as such as multi-tenancy issue, resource allocation, system monitoring and logs, authentication and trust of acquired information and cloud standards [6],[7]. C C must have central components for accountability including responsibility, transparency, remediation and assurance. A simple example of cloud computing is traditional water, electric and gas services and IT services, where they pay for these services in cloud computing. Recently, cloud computing also play a vital role in other technologies such as intelligent transportation system, industries, healthcare, etc[8], [9]. Through cloud computing it is possible to take apart the process of providing the services to end users and adopt existing technologies without any sort of large investments[10].

2. CLOUD COMPUTING ARCHITECTURE

According to NIST, CC possesses the following five important attributes [11]:

- On-demand self-service: at any time the computing resources such as storage, processing, virtual machines etc can be attained from cloud service providers without human interaction.
- Broad network access: heterogeneous devices including mobile phones and laptops can be used to process, store and access resources over a network.
- Resource pooling: service providers can pool their services in cloud and share them with multiple users (called multi-tenancy), where several servers host numerous virtual machines belonging to diverse users.
- Rapid elasticity: any user can frequently avail cloud resources through scale up and scale down based on the increased and decreased computing demands, respectively.
- Measured service: resource usage is monitored through suitable metrics such as CPU hours, storage and bandwidth consumption, etc.

The CC architecture is categorised into different layers depending Infrastructure-as-a-Service, PaaS, and XaaS with embedded CC solutions. Some notable differences exist among deployed CC and types of offered services. These are between computing power and storage space, installed software platforms and online software applications of web-mails to analysis tools. Figure 2 illustrates the typical three layer service model. It is customary to describe briefly the working principle these three layers.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

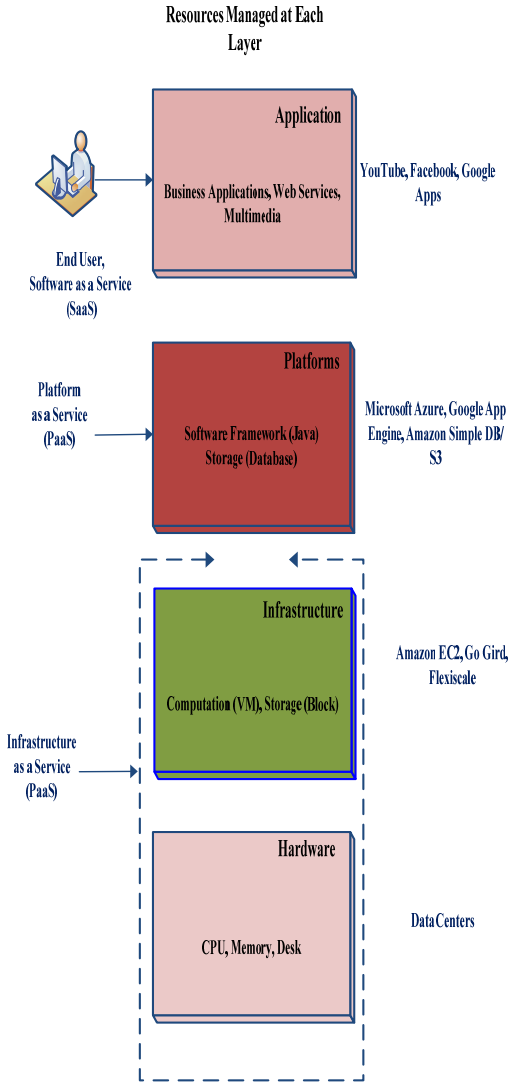

Figure 2: Architecture of CC services.

A. Infrastructure as a Service

Upon request from a provider, the users can avail processor resources, storage, networks and others. This model allows the user to execute and implement applications and operating systems. The user does not intervene the management or control the resources in the cloud, but manages the applications and operating systems for instance Amazon EC2 and Akamai[12],[13]. Typically, the cloud infrastructure services offers a virtual platform to the users as already exists for many years [14]. Customers exploit these facilities and buy resources without configuring expensive servers and data centres, where the charges majorly depend on CPU hour's usage. Users can install, control, manage, and process their own software on cloud virtual machines. These dynamically scalable virtual instances can be rented for long and short time duration depending on customer usage and need. The charges are decided by the usage, where different packages or additional services such as storage and space are offered.

Service providers created data centres worldwide to proffer quick accessibility and prompt services. The web sites are designed to monitor and control cloud services. These services are offered increasingly to individuals and manufacturing companies, where system providers advertise them. These companies stored their useful data in different locations, take backup, synchronize data from different workstations and make them available to web browser (e.g. Rackspace's Cloud Files) [15]. Rackspace and Nirvanix offers online storage solutions for private and corporate users [16]. Another well-known company is Amazon, which offers storage, database solutions, as well as separate service called EC2 instances, Amazon Simple Storage Service (S3), Amazon Elastic Block Store (EBS) and Amazon Simple DB [2].

B. Platform as a Service

Using PaaS model, service providers allow the users to implement their envisioned applications in the cloud by offering different tools and programming languages. However, users are not authorized to intervene the management or control the resources in the cloud with limited access of programming such as Google Apps [17]. In this case, the service provider offers high level software that allows the users to build particular classes of applications and services. The customer exploits provider infrastructure (servers, storage, network, and operating systems) without any management control [18]. Mostly, these services are used for the development of web applications and are programming languages dependent. Customers acquire allocated memory space to test and develop these applications (e.g. Google with Python or Java environment) [19]. Google Applications are freely offered for non-scaling purposes. The Microsoft Azure platform is offered using .NET libraries [20].

C. Software as a Service (SaaS)

In this model, applications are executed on the service provider's cloud infrastructure and accessed through a web browser. Users do not possess remote application, access and responsibilities about infrastructure or physical constitution. Salesforce.com [21], Gmail, and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Facebook belong to this category. For instance, SaaS as a web based e-mail service is an available application in cloud computing. Most of the cloud services being web based are accessed by numerous users through a thin client interface for instant web browsing. Moreover, customers have no rights to manage and control these services except limited user specific configurations authorizations.

3. STATE-OF-THE-ART FOR MODELS OF CLOUD

This section discusses the model of cloud computing. Clouds are categorized on the basis of ownership and cloud data centres as well as multiple or single compromise. Cloud model as displayed in Figure 3 is also distinguished through single and multiple environments. It is worth discussing briefly the classification of single and multiple clouds as well as data centre ownership.

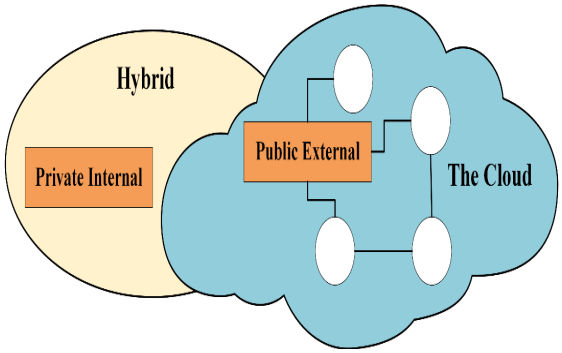

Figure3: Cloud computing models.

3.1 Public Clouds

It refers to a service, where CC is available over the internet for general users. In public cloud the data centres (hardware, and software) are run by third parties, where the services are exposed via internet to other companies such as Amazon, Google, etc. [22]. However, it limits the number of users and only available with pay-as-you-go basis for general public. Thus, there are two types of customers including the end users on the Business-to-Consumers (B2C) market or companies on the Business-to-Business (B2B) market [2].

3.2 Private Clouds

Private cloud refers to any institution possessing their own data centre with several servers, which are greatly dedicated to virtualization, self-provisioning and automated management of resources. The private clouds are beneficial to corporations those invested huge computing power, bandwidth and network storage in improving the utilization of resources. Nevertheless, this model does not enjoy the full economic benefits of CC because the institution needs to maintain the resources even when under-used. Conversely, the private cloud being owned by single company is only authorized for the total control over all the infrastructure and applications [22]. The private cloud also relies on virtualization and increases their utilization [22]. It is worth mentioning that virtualization and full control on infrastructure is the primary advantage of private CC.

3.3 Hybrid Clouds

The hybrid model being the combination of private and public clouds allows one to choose and run both the environment. This model also provide the facility to run some applications on private cloud and some on the public cloud as demonstrates in Figure 3 [23]. These scalable IT resources and cloud facilities often benefit many companies in terms of their data storage and specific applications with absolute security. However, hybrid models are unsuitable for complex databases and for synchronization due to their inherent complexity in distributed applications across different environments [23].

3.4 Community Cloud

Community cloud extends the concept of the private cloud by incorporating multiple customers with shared concerns. Some characteristics of this cloud are similar to private one. One particular example of a community cloud is the health care [23]. Recently, Tech Target 9 reported that a major collaboration among different organizations such as Open Science Data Cloud and the University of Chicago's Institute of Genomics and System Biology, Centre for Research Informatics, and Institute of Translational Medicine established the Bio-nimbus Protected Data Cloud (PDC) [2]. The PDC is a cloud-based infrastructure (open source petabyte-scale) built to manage, analyse, and provide easy access of large genomic datasets to the research community (under the Cancer Genome Atlas (TCGA)) in a secured and submissive manner. The TCGA uses techniques to determine mutations that cause cancer and the PDC allows the authorized researchers to access TCGA data bank. This is an excellent example of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the community cloud, where collaboration of different stakeholders with a common interest became feasible. Through authorization process the trusted parties can access the data to achieve success for future development of cancer medicine [1].

4. PROS AND CONS OF CC

Currently, CC became attractive due to its escalating prospect to bring a radical change in the industries. Several striking attributes such as storing data online instead of physical hard drive in traditional storage systems, flexibility of data access from anywhere and anytime, and reduced cost of extremely powerful IT operations make CC fashionable [24]. Here we discuss some advantages and of CC.

4.1 Advantages of CC

- Mobility: In the era of global market and economy, CC provides the ultimate mobility to the users to coping up with market developments and stays connected with tools and data round the clock at any place. The old traditions, where users are supposed to make telephone calls to get regular reports are not feasible anymore. Recent advancement in CC assisted internet connectivity worldwide has truly enhanced the users mobility [25].
- Versatile Compatibility: CC can provide identical services to all users due to its flexible operating system or software platform. Furthermore, it is efficient to save users efforts and reduce difficulties through available platforms via cloud applications irrespective of systems types [23].
- Affordability: In CC, users only pay for the used storage and services they need unlike other computing techniques, where whole package with unnecessary applications and expensive solutions need to be purchased [24].
- Individuality: One of the most important features of CC is its compatibility with any kind of companies, where the individuality is maintained despite of using the CC services in user defined preferred ways [24].
- Cost Savings: Through CC companies cut-down their operational and other expenditures simultaneously enhance their capabilities in terms of services and technologies. Using little physical resources and infrastructures, companies can fulfil their needs and gain in-house IT resources [24].
- Scalability/Flexibility: CC is flexible in adoption, terminable as and when required and expandable services growth. Furthermore, during peak time companies can enhance their capacity and use additional services to satisfy the customers demand [24].
- Reliability: Cloud services are reliable with multiple sites, where it supports individuals and businesses continuously with secured data recovery in disastrous situations [23].
- Maintenance: CC requires minimal system maintenance with available access through different application program interfaces (APIs). The services do not use any sort of installation in PC and users can easily reduce maintenance requirements [23].

4.2 Disadvantages of CC

- Availability of Service: There is occasional disruption of availability in the services. For continuous services without any delay or interruption the ideal solution may be the implementation of multiple clouds. The occurrence of distributed denial of service (DDOS) attacks is another demerit. Utility companies address these obstacles through elasticity, where CC moves from attack path to SaaS. However, it should have DDOS protection as a central component.
- Data Lock-In: The improper standardization of APIs in CC prohibits the customers to extract program and data between different sites. This problem can be overcome by developing a standard for APLs, where SaaS developer use services and data through multiple CC. Upon failure of a particularly company, all copies of consumer data will not be removed completely. The APLs standardization enables the "Surge Computing" that enhances the efficiency in heavy workload with easy running.
- Data Confidentiality and Auditability: This disadvantage of CC can be surmounted through the handle of well designed technologies such as encrypted storage, packet filters and VLAN (virtual local area networks) firewalls. Auditability refers to an additional layer behind the virtualized guest OS that is able to provide enhanced security. Some national laws are outlined through Geographical Data Storage. These laws are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

available for some countries such as Amazon services, in Europe and USA.

- Scalable Storage: A scalable storage store is needed to handle resource management, data durability, scalability and high availability.
- Bugs in Large Distributed Systems: Removal of errors from distributes systems is a key challenge, where some solutions relying on virtual machines are proposed[22].
- Security, Privacy and Integrity: Certainly, these are the grave concerns towards CC implementation [2]. A recent studies survey over 500 IT managers belongs to 17 different countries revealed the benefits of CC. However, they showed their confidence in internal cloud-based systems due to threats safety and enhance information control [26]. An investigation by the International Data Corporation on 244 IT managers revealed that 74.6% of respondents are doubtful about the security of CC. However, this problem can be minimized with data encryption, compliance with standards, and service level agreements [26].

5. PRESENT CHALLENGES IN CC

CC opened several new research avenues with the diverse environment, open research issue and challenges. The main issues in CC are security, privacy, scalability, integrity, auditability, etc. For comfortable and enjoyable cloud services, considerable assurance is required in terms of reliance, availability, and security. Security and privacy of a cloud shall remain a matter of wide research in coming years. The migration of sensitive data and applications to the cloud has raised issues with security and privacy. Despite the many benefits of CC, businesses and organizations are still unwilling to move to the cloud. The delayed growth of CC market is mainly due to the lack of assurance in Privacy Preserving Data Mining (PPDM). Consumers are anxious about storage, networks, and virtualization with regard to security and privacy. Data privacy concerns are more important now than ever with the rise of big data analysis. Large amounts of data collected in different spheres can be used for data mining to enable better decision making. Certain sensitive data could contribute positively to data mining by both government and non-government organizations for research purposes. Some multifaceted research would produce more fruitful results with analysis of data sets such as censuses, hospital records, voter registration records, or customer service records. But there is undoubted that cloud computing has a bright future waiting for it.

5.1 Cloud Security

The data maintenance and services in CC system are provided in such a way the client/customer remains totally unaware of the data handling and storage procedures. Actually, the client has no control over service level agreements (SLA's) such as performance management, definition of services, customer duties, problem management, warranties and remedies, responsibilities, disaster recovery, security, business continuity disaster and termination [27] and [28]. A survey about different security risks and threats related to cloud system is presented by Subashini et al. [29][30][31]. The importance of cross-site scripting (XSS), network penetration, access control weaknesses and packet analysis session etc in CC are discussed. In their report, major issues connected to data security, locality, segregation, integrity, access, tenant, authentication, authorization, confidentiality, breaches virtualization vulnerability, identity network security, backup management, sign-on process and web application security are emphasized. Zhou et al, examined five aspects of cloud system such as privacy, accessibility, regularity, data reliability and audit for security [32]. It is acknowledged that major privacy issues in cloud services including multi-tenancy, system monitoring and logs, resource location, authentication and trust of acquired data and cloud standards require special attention [6], [7].

Central components for accountability, transparency, remediation and guarantee are essential in CC. Incorporation of ACPS (advanced cloud protection system) for the enhanced protection of the cloud system is proposed [33], which is able to monitor both middleware and guest integrity to provide security from different types of attacks. However, system remains fully transparent and interacts with users and service providers. The proposed system can notify the security management layers and locally reacts with the security breaches or attacks. Sadeghi et al. presented a model and discussed numerous possible architectures for outsourcing data and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

arbitrary computations which can deliver reliability, privacy and verifiability[34]. The first architecture calculates the function within a tamper-proof hardware token and the second one works on fully holomorphic encryption. Conversely, the third architecture combines the advantages of the formers and disables their individual shortcomings.

The primary risks in CC arise due to sharing of physical infrastructure among mutual distrustful clients [35]. Ristenpart et al. [35] highlighted several approaches to mitigate this particular risk. Cloud providers can mystify both the placement policy and internal structure of services to confound adversary's attack by placing a virtual machine (VM) on the physical device as its target. The providers may focus on the side-channel susceptibilities and apply blinding techniques to reduce the trickled information. It is asserted that such options are only foolproof solution to the phishing attacks as demanded by clients with high privacy requirements. Gowrigolla et al. [36] proposed a data protection approach together with public auditing and some of the unique factors. This is comprised of four algorithms including KeyGen, GenProof, SigGen, and VerifyProof. The first algorithm (KeyGen) generates keys and runs on the client side for setup the scheme [36]. The SigGen algorithm verifies the metadata by the client, which consists of some other information and signatures used for auditing purposes. Cloud server providers set up GenProof to produce data storage correctness verification. Conversely, the VerifyProof is used through TPA for auditing the evidence from the cloud server.

Hamlen et al., discussed the storage and data layers [37], where different approaches for securing the published documents of third parties on cloud system is outlined. A secure cloud is developed with hardware components of 800 TB data storage, 2400 GB memory and many commodity computers. Software including Hadoop and data as a semantic web repository are also used. The proposed cloud system renders efficient support for storing encrypted sensitive data, strong authentication, fine-grained access control and also able to make query as well as manages enormous amounts of data. In short, vast amount of recent literatures repeatedly emphasized the cloud security issues as major concern. The rapid progress in CC system is attempted to develop some robust techniques to manage the required requirements of cloud environments. Yet, clients might not be satisfied with the CC technology due to security issues which are needed to be settled as top priority. All these previously developed architectures must be improved radically to achieve a strong secured cloud.

5.2 Cloud Privacy

Recently, Sun et al. acknowledged the key issues related to security, secrecy and reliance on CC systems [38][39]. The tangible and intangible threats related to cloud systems are discussed in details to make the clients aware of these types of security, privacy, and reliance threats. Different mechanisms are used to eliminate these threats and provide a secure, trustworthy, and reliable CC system. Tchifiionova et al. described the security and privacy as persisting threats on cloud systems unless clients fully comprehend the cloud system management, its working principle. It is also important for the users to understand whether the organization or business leak their private information and data to get lost in the cloud [40]. Xiao et al., discussed five most representative attributes related to security and privacy of cloud system such as accessibility, secrecy, accountability, reliability and privacy, preservation [41]. The relationships among these parameter, the vulnerabilities misused by attackers, the threat models, and existing defence strategies in a cloud scenario are described. It is affirmed that the privacy must not be isolated from the security due to its significance in cloud system. Privacy is strongly related to security and the security attributes positively or negatively impacts on the privacy. Issues regarding the data protection on CC system suggest that some privacy laws must be enforced [42][43]. It is concluded that cloud system must possess high level regulatory recommendations data protection, risk allocation, security, transfer, intellectual property, confidentiality and non-disclosure, law enforcement access and limitation of liability in change of control, and audit.

Wayne et al. developed a measurement system based on standardized dimensions to assess privacy risks in cloud environments. The drawbacks of current techniques applied in cloud computing systems are described [44]. Svantesson et al. identified the severe risks of consumer rights and privacy in CC systems. It is asserted that the current privacy law can settle some of these threats [45]. Nandipati et al.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

introduced a new cloud framework known as Data Protection as a Service, which is able to reduce the per-application development efforts dramatically as required for data protection. Meanwhile, it also allows the rapid development and maintenance [46]. The DPaaS (Data Protection as a Service) paradigm offers logging and auditing at the platform level to share the advantages of all applications running on top. Sykes et al., presented a model based on three distinct logical components including the privacy service mediator (PSM), mobile device agent (MDAg), and cloud services [42]. Using the PSM, the communication between mobile applications and cloud services is proposed. It analyzed the exchange of information in privacy perspective. Following a command design pattern, the mobile application can bundle the cloud-service calls into a chain of command objects which are linked and sent to PSM for execution via MDAg.

Based on the description logic of transforming the pre-negotiation of privacy policy for decidable issue of Tableau algorithm, Ke et al. built a privacy negotiation model between service provider and user on the [47]. The privacy policy negotiation is composed of two steps. Firstly, Tableau algorithm of description logic is used by detecting the conflicts of privacy attribute collections, where the privacy knowledge base (PKB) is obtained to satisfy user requirements. Secondly, both user and service provider privacy policy requirements are achieved through ordinal exchange of privacy disclosure assertion based on privacy attribute sequences between user and service provider. Later, two types of secure CC (SCC) systems are proposed [48]. One of them is with the trusted third party (TTP) and the other is without it. The main objective of these schemes is to address data security threats in the cloud server. The symmetric property in secret sharing is added, which successfully reduced the cost of sharing between the client and the server. By the homomorphism property of secret sharing, SSC is extended to multi-server SCC (MSCC) fitting in the multi-server environment. Compared to the previous data privacy by authentication and secret sharing (PASS), these schemes achieved better security and performance.

Song et al. presented a new framework for confidentiality protection of private data and recovery services known as parity cloud service [49]. Parity cloud service provides solution for all problems related to cloud system such as consistency, economical efficiency, accessibility, and confidentiality while developing personal data recovery service. The proposed approach is simple and does not involve with any privacy protection resources. It works on collaboration-based data recovery algorithm, in which the data loss rate is minimal. Wang et al. proposed a privacy-preserving public auditing system for security of stored data on cloud system [50], where TPA (third party auditing) performs audit for stored data without any damage of data copy. In the proposed system a random mask and holomorphic authenticator techniques are used to ensure TPA without any information regarding the data content stored on the cloud system while running the auditing process. The careful performance and security analysis revealed that the proposed frameworks are safer and highly efficient. It is asserted that the security and high efficiency of proposed frameworks may shed light on economies of scale for CC.

Lu et al. presented a scheme from avoiding the cloud server to learn any possible sensitive plaintext in the outsourced databases [21]. Furthermore, the proposed scheme also provided private querying so that neither database holder nor the cloud server can access the query details. Additional conditions such as client's input are authorized by cloud auditing (CA). An encryption scheme is incorporated to protect data secrecy and permit access control. It is developed to retrieve search token and decryption key for a user from database owner without showing query contents. This scheme suffers from many shortcomings such as it only supports equality testing and hides concrete contents in the conditional expression, and it does not support the joint operations between two tables. Schiering et al. addressed a prototype of an IaaS cloud service, which serves on the basis of SaaS compliant with European directive [51]. This is achieved by a combining the organizational and technical measures accompanied by auditing and monitoring.

Briefly, all these studies clearly indicated the exponential growth of privacy risk exposure to the enterprise. In one school of thought it is believed to separate privacy from security due to its particular significance in cloud systems. Several CC system providers are concerned about security and privacy problems. They distinguished the appropriate solution in five facets such as availability, data integrity,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

confidentiality, control, and audit for privacy. Some of them found that for some information the business clients are concerned with sharing private litigants and Government agencies. It may hack their private data more easily from a third party as compared to the creator of the data. Analyses revealed that privacy is a complicated issue and it is required to merge different approaches to generate a comprehensive solution that does not compromise client's privacy. Figure 4 illustrate the cloud security and privacy.

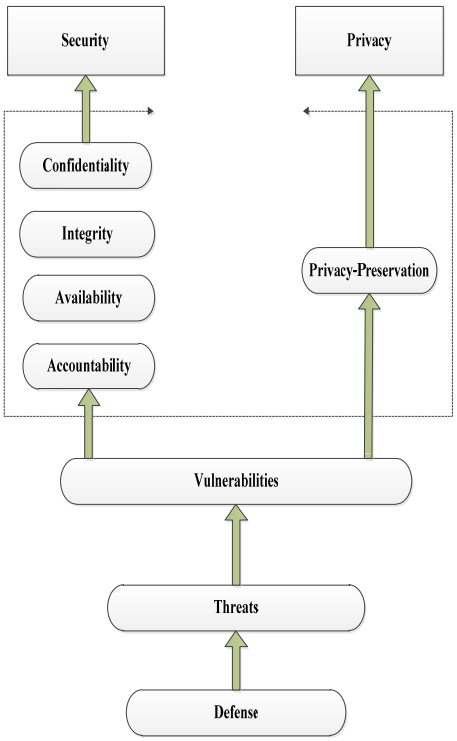

Figure 4 Cloud security and privacy

6. DISCUSSION

There are several survey papers on cloud computing. My work addresses the same area, but, from a different perspective. I surveyed the cloud computing and categorized based on its architecture, its models, pros and cons of cloud computing and focuses on the most important recent challenges of cloud computing. Furthermore, I present the categorization of current studies in Table 1. I mapped the literature review of cloud computing as shown in Figure 1.

Table 1: The Categorization of Current Studies of Cloud Computing

References	Cloud Computing	Cloud Computing Architectures	Models Of Could	Pros And Cons Of Cloud Computing	Present Changeless of Cloud Computing
[1] R. Samani et al.	√		√		
[2] A. Fox et al.	√		√	√	
[3] Mell and T. Grance.	√				
[4]S. Pearson and A. Charlesworth.	√				
[5]M. Williams et al.	√				
[6]C. Rong et al.	√				
[7]Z. Mahmood.	√				
[8]K. N. Qureshi and A. H. Abdullah.	√				
[9]K. N. Qureshi et al.	√				
[10]D. Catteddu and G. Hogben.	√				
[11]A. K.-H.		√			

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Ilango Sriram.					
[12]L. Youseff et al.		√			
[13]A. Cardoso and P. Simões,		√			
[14]D. Hilley		√			
[15]H. Abu-Libdeh et al.		√			
[16]E. Deelman et al.		√			
[17]A. Lenk et al.		√			
[18]C. N. Höfer and G. Karagiannis		√			
[19] R. Buyya et al.		√			
[20]V. Khanaa et al.		√			
[21] Y. Lu and G. Tsudik		√			
[22] F. D. Ahmed and A. Al Nejam		√	√		
[23]U. Kumar and A. Jangra.			√	√	
[24]S. Zhang et al.				√	
[25]M. Singh et al.				√	
[26]W. Sun et al.				√	
[27]B. R. Kandukuri et al.					√
[28]S. Srinivasamurthy and D. Liu.					√
[29]S. Subashini and V. Kavitha					√
[30]A. Bisong et al.					√
[31]G. Kulkarni et al.					√
[32]M. Zhou et al.					√
[33]F. Lombardi and R. Di Pietro.					√
[34]A. Sadeghi et al.					√
[35]T. Ristenpart et al.					√
[36]B. Gowrigolla et al.					√
[37]K. Hamlen et al.					√
[38]D. Sun et al.					√
[39]R. Gellman.					√
[40]V. Tchifilionova.					√
[41]L. Y. Xiao					√

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

et al.					
[42]S. Porwal et al.					√
[43]N. J. King and V. Raja.					√
[44]W. a J. Pauley					√
[45]D. Svantesson and R. Clarke					√
[46]B. L. Nandipati and G. Sridevi.					√
[47]C. Ke et al.					√
[48]C.-N. Yang and J.-B. Lai.					√
[49]C.-w. Song et al.					√
[50]H.-j. Wang et al.					√
[51]I. Schiering and J. Kretschmer.					√

7. CONCLUSION

This paper comprehensively reviews the past development, recent progress and future trends in CC by emphasizing CC challenges, merits, demerits and security concerns. Various IT companies change their trend into CC services. Undoubtedly, CC is an efficient solution for different businesses with tremendous future prospects, which is evident from various companies trend to switch from traditional technologies to CC. CC is well-intentioned and attractive solution for enterprises and for individuals to build their system with more profitable, cost effectiveness and scalable way. Therefore, the impact of CC on ISV is positive for all level of users including IT managers, engineers, developers and management. The scope of CC advancement is phenomenon because it overcomes the maintenance, installation, and hurdles. This new technology is prospective in terms of opening several new avenues for learning and career development. The extent of CC is exponentially growing and the services models are bringing a revolutionary change in the Internet. It also announced a low cost supercomputing facilities and services for users to provide accessibility, processing, virtualization, storage, etc. However, many issues related to security, availability, etc. need special attention before it penetrates and dominates the global market. This panoramic overview is expected to provide the researchers a basic understanding on the current challenges and development in the field of CC.

The capability-based reviewed of the studies of cloud computing has helped to identify the Cloud areas that are better addressed by these categorized and more importantly the areas that are lacking support so that future research can take them into consideration. The review in this paper have provided a comprehensive overview of cloud computing. I consider this part of work as a reference and a basis for further research work in this area in the future.

REFERENCES:

[1] R. Samani, B. Honan, and J. Reavis, "CSA Guide to Cloud Computing," in CSA Guide to Cloud Computing Implementing Cloud Privacy and Security, Elsevie, 2015, pp. 1–22.

[2] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, p. 50, 2009.

[3] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," Nist Spec. Publ., vol. 145, p. 7, 2011.

[4] S. Pearson and A. Charlesworth, "Accountability as a way forward for privacy protection in the cloud," in Lecture Notes in Computer Science (including subseries

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009, vol. 5931 LNCS, no. December, pp. 131–144.

[5] M. Williams, A Quick Start Guide to Cloud Computing: Moving Your Business Into the Cloud. Kogan Page, 2010.

[6] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Computers & Electrical Engineering, 2013, vol. 39, no. 1, pp. 47–54.

[7] Z. Mahmood, "Data location and security issues in cloud computing," in Emerging Intelligent Data and Web Technologies (EIDWT), 2011 International Conference on, 2011, pp. 49-54.

[8] K. N. Qureshi and A. H. Abdullah, "A Survey on Intelligent Transportation Systems," Middle-East J. Sci. Res., , 2013, vol. 15, no. 5, pp. 629–642.

[9] K. N. Qureshi, A. H. Abdullah, and F. Computing, "Adaptation of Wireless Sensor Network in Industries and Their Architecture , Standards and Applications," , 2014, vol. 30, no. 10, pp. 1218–1223.

[10] D. Catteddu and G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," in Web Application Security, vol. 72, no. 1, Springer Berlin Heidelberg, 2009, pp. 17-17.

[11] A. K.-H. Ilango Sriram, "Research Agenda in Cloud Technologies," arXiv:1001.3259, 2010.

[12] L. Youseff, M. Butrico, and D. Da Silva, "Toward a unified ontology of cloud computing," in Grid Computing Environments Workshop, 2008. GCE '08, pp. 1 – 10.

[13] A. Cardoso and P. Simões, "Cloud computing: Concepts, technologies and challenges," in Communications in Computer and Information Science, 2012, vol. 248 CCIS, pp. 127–136.

[14] D. Hilley, "Cloud Computing : A Taxonomy of Platform and Infrastructure-level Offerings," Georgia Institute of Technology, Tech. Rep, 2009, no. April, pp. 1–37.

[15] H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon, "RACS: a case for cloud storage diversity," in Proceedings of the 1st ACM symposium on Cloud computing, 2010, pp. 229–240.

[16] E. Deelman, G. Singh, M. Livny, B. Berriman, and J. Good, "The cost of doing science on the cloud: The montage example," in 2008 SC - International Conference for High Performance Computing, Networking, Storage and Analysis, SC 2008, pp. 1 – 12.

[17] A. Lenk, M. Klems, J. Nimis, S. Tai, and T. Sandholm, "What's inside the Cloud? An architectural map of the Cloud landscape," in Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009, pp. 23-31.

[18] C. N. Höfer and G. Karagiannis, "Cloud computing services: Taxonomy and comparison," J. Internet Serv. Appl., 2011,vol. 2, no. 2, pp. 81–94.

[19] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on, 2008, pp. 5-13.

[20] V. Khanaa, K. P. Thooyamani, and R. Udayakumar, "Modelling Cloud Storage," World Appl. Sci. Journal, 2014, vol. 129, no. 14, pp. 190–194.

[21] Y. Lu and G. Tsudik, "Enhancing data privacy in the cloud," in IFIP Advances in Information and Communication Technology, 2011, vol. 358 AICT, pp. 117–132.

[22] F. D. Ahmed and A. Al Nejam, "Cloud Computing : Technical Challenges and CloudSim Functionalities," IInternational J. Sci. Res., vol. 2, no. 1, p. 5, 2013.

[23] U. Kumar and A. Jangra, "A Review Paper on Cloud Computing," Int. J. Inf. Technol. Knowl. Manag., no. ICFTEM-2014, pp. 74–77.

[24] S. Zhang, S. Zhang, X. Chen, and X. Huo, "Cloud Computing Research and Development Trend," in Future Networks, 2010. ICFN '10. Second International Conference, pp. 93–97.

[25] M. Singh, J. S. Bhatia, and D. Malhotra, "Big Data : The Future of Data Storage," IOSR J. Comput. Eng. (IOSR-JCE), 2014, vol. 16, no. 5, pp. 130–136.

[26] W. Sun, W. Lou, Y. T. Hou, and H. Li, "Privacy-Preserving Keyword Search Over Encrypted Data in Cloud Computing," Secur. Cloud Comput. Springer New York, 2014., pp. 189–212.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[27] B. R. Kandukuri, V. R. Paturi, and A. Rakshit, "Cloud security issues," in Services Computing, 2009. SCC'09. IEEE International Conference on, 2009, pp. 517-520.

[28] S. Srinivasamurthy and D. Liu, "Survey on cloud computing security," in Proc. Conf. on Cloud Computing, CloudCom, 2010.

[29] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications. Elsevier, 2011, vol. 34, no.1. pp. 1–11.

[30] A. Bisong, Syed, and M. Rahman, "An Overview of the Security Concerns in Enterprise Cloud Computing," Int. J. Netw. Secur. Its Appl., 2011, vol. 3, no. 1, pp. 30–45.

[31] G. Kulkarni, J. Gambhir, T. Patil, and A. Dongare, "A security aspects in cloud computing," in Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on, 2012, pp. 547-550.

[32] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on, 2010, pp. 105-112.

[33] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," Journal of Network and Computer Applications, Jul. 2011,vol. 34, no. 4, pp. 1113–1122.

[34] A. Sadeghi, T. Schneider, M. Winandy, and G. Horst, "Token-Based Cloud Computing,", in Trust and Trustworthy Computing, ed: Springer, 2010, pp. 417-429.

[35] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 199-212.

[36] B. Gowrigolla, S. Sivaji, and M. R. Masillamani, "Design and auditing of cloud computing security," in Information and Automation for Sustainability (ICIAFs), 2010 5th International Conference on, 2010, pp. 292-297.

[37] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security Issues for Cloud Computing," Int. J. Inf. Secur. Priv., 2010,vol. 4, no. 2, pp. 39–51.

[38] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments," Procedia Engineering, 2011, vol. 15, pp. 2852–2856.

[39] R. Gellman, "Privacy in the clouds: risks to privacy and confidentiality from cloud computing," in Proceedings of the World privacy forum, 2009, pp. 1–26.

[40] V. Tchifilionova, "Security and privacy implications of cloud computing–Lost in the cloud," in Open Research Problems in Network Security, ed: Springer, 2011, pp. 149-158.

[41] L. Y. Xiao, Z. Wang, R. Wang, and H. N. Wang, "Architecture and Key Technologies of Cloud Computing," Advanced Materials Research, 2013, vol. 756, pp. 1953-1956.

[42] S. Porwal, S. K. Nair, and T. Dimitrakos, "Regulatory Impact of Data Protection and Privacy in the Cloud," in Trust Management V, ed: Springer, 2011, pp. 290-299.

[43] N. J. King and V. Raja, "Protecting the privacy and security of sensitive customer data in the cloud," Computer Law & Security Review, 2012, vol. 28, pp. 308-319.

[44] W. a J. Pauley, "An Empirical Study of Privacy Risk Assessment Methodologies in Cloud Computing Environments," Nova Southeastern University, 2012.

[45] D. Svantesson and R. Clarke, "Privacy and consumer risks in cloud computing," Computer Law & Security Review, , 2010, vol. 26, pp. 391-397.

[46] B. L. Nandipati and G. Sridevi, "A Novel Computing Paradigm for Data Protection in Cloud Computing," IJMER, 2013, vol. 3, no. 4, pp. 2498–2501.

[47] C. Ke, Z. Huang, and M. Tang, "Supporting negotiation mechanism privacy authority method in cloud computing," Knowledge-Based Systems, 2013, vol. 51, pp. 48-59.

[48] C.-N. Yang and J.-B. Lai, "Protecting data privacy and security for cloud computing based on secret sharing," in Biometrics and Security Technologies (ISBAST), 2013 International Symposium on, 2013, pp. 259-266.

[49] C.-w. Song, S. Park, D.-w. Kim, and S. Kang, "Parity cloud service: a privacy-protected personal data recovery service," in Trust, Security and Privacy in Computing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and Communications (TrustCom), 2011 IEEE 10th International Conference on, 2011, pp. 812-817.

[50] H.-j. Wang, C.-a. Hu, and J.-s. Liu, "Distributed mining of association rules based on privacy-preserved method," in Information Science and Engineering (ISISE), 2010 International Symposium on, 2010, pp. 494-497.

[51] I. Schiering and J. Kretschmer, "The Infrastructure Level of Cloud Computing as a Basis for Privacy and Security of Software Services," in Privacy and Identity Management for Life, ed: Springer, 2012, pp. 88-101.