Cloud Computing Features, Issues and Challenges: A Big Picture

Deepak Puthal*, B. P. S. Sahoo†, Sambit Mishra‡, and Satyabrata Swain‡
*Dept. of Computer Science and Engineering, National Institute of Technology Silchar, India
†Dept. of Computer Science and Information Engineering, National Central University, Taiwan (R. O. C.)
‡Dept. of Computer Science and Engineering, National Institute of Technology Rourkela, India
Email: {deepak.puthal, biswap.singh, skmishra.nitrkl, satya.swain10}@gmail.com

***Abstract*—Since the phenomenon of cloud computing was proposed, there is an unceasing interest for research across the globe. Cloud computing has been seen as unitary of the technology that poses the next-generation computing revolution and rapidly becomes the hottest topic in the field of IT. This fast move towards Cloud computing has fuelled concerns on a fundamental point for the success of information systems, communication, virtualization, data availability and integrity, public auditing, scientific application, and information security. Therefore, cloud computing research has attracted tremendous interest in recent years. In this paper, we aim to precise the current open challenges and issues of Cloud computing. We have discussed the paper in three-fold: first we discuss the cloud computing architecture and the numerous services it offered. Secondly we highlight several security issues in cloud computing based on its service layer. Then we identify several open challenges from the Cloud computing adoption perspective and its future implications. Finally, we highlight the available platforms in the current era for cloud research and development.**

***Keywords*-Cloud computing; Cloud security; Virtualization; Workflow scheduling; Data integrity, Public auditing.**

I. Introduction

In recent years, the popularity and rapid growth in processing and storage technologies and the success of the Internet, computing resources have become cheaper, more powerful and more ubiquitously available than ever before [1]. This technological trend is popularly known as cloud computing and has led to an evolutive way to provide a better answer to current and future information and communication technology (ICT) requirements. Cloud computing gives an adaptable online environment which encourages the capability to handle an expanded volume of work without affecting on the execution of the framework. With the advent of Cloud, the increasing number of cloud providers and the variety of service offerings have made it difficult for the researcher and pose numerous challenges to cope with. Over the years, researchers are working around the world to enable this technology towards wide business opportunity and in other areas of IT infrastructure, utilizing the cloud computing services and mechanism.

Utilization of cloud services makes a developing relationship among both public and private sector substances and the people served by these elements. Cloud computing is attractive to business owners as it eliminates the requirement for users to plan ahead for provisioning, and allows enterprises to start from the small and increase resources only when there is a rise in service demand [2]. Promoting and expanded expansion of cloud offers made a vast build-up around the cloud that led to strong user expectation pressure, that partially couldn't be reasonably be satisfied - this is by and large the case for any promising technologies or concepts. Marketing tends to guarantee attributes that are effortlessly confounded with qualities with distinctive implications in different domains, possibly prompting the confusion towards cloud. Consequently, thorough characterization of cloud application features is an essential for the further improvement of cloud framework.

Over the years, several technologies such as virtualization, grid computing, and service-oriented architecture (SOA) have matured and significantly contributed to making cloud computing viable [5]. On the other hand, cloud computing is still in infancy and experiences absence of institutionalization in many aspects. In current scenario, most new cloud providers propose their own solutions and proprietary interfaces for access to resources and services which lead to the heterogeneity problem and raises barriers to cloud realization. As users get more experienced in using cloud infrastructures, their capabilities, strengths and deficiencies become more and more apparent. The cloud providers are thus working under growing pressure to fulfil the promises, and provide better services to their users.

As cloud infrastructure is being used throughout the globe, security is the major concern. This sharing of framework together to the way that the customers to the cloud have needed control over the cloud foundation raises huge security worries. The clouds have a different architecture based on the services they provide. The information is stored on to a concentrated area called server farms having a huge size of information store and those data process in the server. So, the customers need to trust the cloud resource provider on the accessibility and additionally information security. The service level agreements (SLA) is the only legal agreement between the service provider and client. The only means the supplier can addition trust of the client is through the SLA, so it must be institutionalize.

Looking at the current trends and overgrowing interest for this subject, this paper explores the current patterns in the space of Cloud computing and presents researching space for future improvements of this technology. Key elements of opportunity in cloud research are provided, and each one of them explained in detail.

The rest of the paper is organized as follows. Section II

presents a study on the cloud computing architecture and highlights the recent available computing tools. In section III, we list out several security issues in cloud computing. We pinpoint the open challenges and discuss its future implication in section IV. Finally in Section V, we conclude the paper.

II. Cloud Computing Architecture

A. The definitions

The term distributed computing appears to start from machine system standard that speak to the web as a cloud. A large portion of the real IT organizations and market research firms such as IBM (2009), Sun Microsystems (2009), Gartner by Plummer et al. [6], Forrester Research by Staten [7] and Buyya et al. [9] have produced white-papers that effort to define the meaning of cloud computing. These discussions are basically reaching an end and a typical definition is beginning to develop. The US National Institute of Standards and Technology (NIST) has created a working definition that blankets the generally concurred parts of cloud computing. The NIST defines cloud computing as, 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 [8]. This NIST definition describes cloud computing as having five essential characteristics, three service models, and four deployment models [2].

B. The essential characteristics of cloud computing [2] [8]

- On-demand self-service: Registering could resources be gained and utilized whenever without the requirement for human association with cloud administration suppliers.Computing resources include processing power, storage, virtual machines, etc.
- Broad network access: The beforehand said resources could be gotten to over a system utilizing heterogeneous gadgets, for example, laptops or mobiles telephones.
- Resource pooling: Cloud administration suppliers pool their resources that are then imparted by numerous clients. This is alluded to as multi-tenure where, for instance, a physical server may have a few virtual machines having a place with distinctive clients.
- Rapid elasticity: A client can rapidly gain more resources from cloud by scaling out and can scale back in by discharging those resources once they are no more needed.
- Measured service: Resources utilization is measured by monitoring storage usage, CPU hours, bandwidth usage, etc. The said metrics are applied to all clouds, but each cloud provides users with services at a different level of abstraction, which is an alternate to an administration.

C. The three most common service models of cloud computing

A cloud can collaborate with customer/client in a mixed bag of courses, through capacities called services. Across the web, three major types of models, of services have emerged, Fig. 2 shows the details of cloud computing service model.

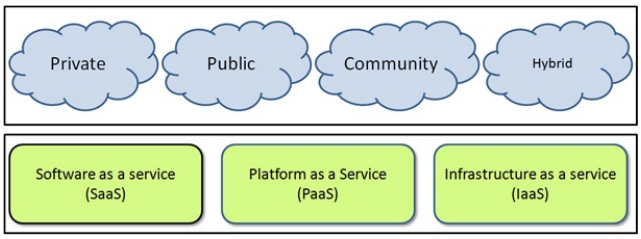

Fig. 1. Cloud solutions based on the system's deployment and service model.

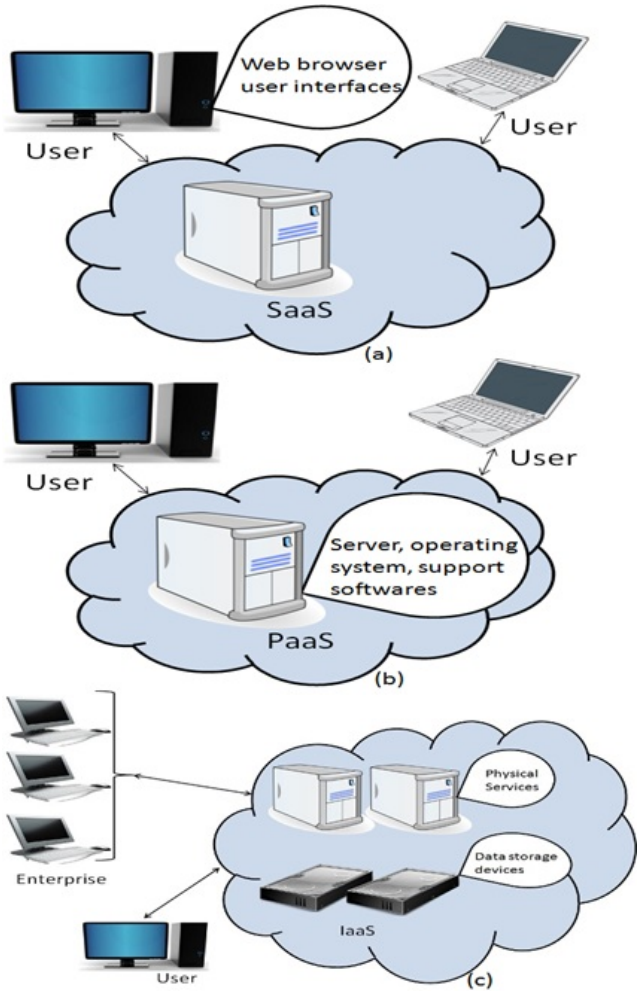

Fig. 2. Service model of Cloud: (a) Software as a service (SaaS), (b) Platform as a Service (PaaS), and (c) Infrastructure as a service (IaaS).

Software as a service (SaaS): Provides consumer the capability to use applications running on a cloud infrastructure mainly on the web browser to access software that offer as a service over the web. The consumer do not have control or figure out how to the underlying framework including system, servers, network, operating systems, storage, or even individual application capacities, with the conceivable exemption of constrained client particular application setup settings.

GoogleDocs[1] and Salesforces[2] are prominent examples.

Platform as a Service (PaaS): Provides the capability to deploy onto the cloud infrastructure, consumer created applications, produced using set of programming languages and tools that are supported by the Paas provider. The consumer does not oversee or control the underlying cloud framework including network, servers, operating systems, or storage, yet has control over the sent applications and conceivably application facilitating environment arrangements. Much the same as the Saas model, clients do not have control or access to the underlying base being utilized to have their applications at the Paas level.Examples of PaaS are Google App Engine[3] and Microsoft Azure[4] are prominent examples that use the PaaS model of cloud computing.

Infrastructure as a service (IaaS): Provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources from an IaaS provider, and allow the consumer to deploy and run any software, which can include operating systems, services and applications. The client has control over operating systems, storage, deployed applications and perhaps constrained control of select systems administration parts. Rather than the Paas model, the Iaas model is a low level of reflection that permits clients to the right of the entrance the underlying foundation through the utilization of virtual machines. Iaas gives clients more adaptability than Paas as it permits the client to convey any product stack on top of the operating system. Examples of IaaS are Amazon Web Services EC2 and S3[5] are prominent examples that use the IaaS model of cloud computing.

D. The four deployment models of cloud computing

A cloud organization model indicates how resources inside the cloud and shared. Fig. 1, shows four different cloud deployment models: private cloud, public cloud, community cloud, and hybrid cloud. Each model impacts the comparing scalability, reliability, security, and cost.

Private cloud: A cloud that is used exclusively by one organisation, company, or one of its customers. The cloud may be operated by himself or a third party, private cloud offers increased security at greater cost. The St. Andrews Cloud Computing Co-laboratory[6] and Concur Technologies (Lemos, 2009) are illustration associations that have a private cloud.

Public cloud: A cloud that can be used by general public. Due to its openness the cloud may be less secure. Public cloud is the best option with less expensive. This can be a large organization and offer services. Public clouds require significant investment and are usually owned by large corporations such as Microsoft, Google or Amazon.

Community cloud: A cloud that is shared by two or more several organizations or company and is usually setup for their specific requirements. This is typically for the shared concern (e.g. such as schools within a university).

Hybrid cloud: A cloud that setup using a mixture of two or more private, public, or community cloud. In the hybrid cloud could be freely overseen yet applications and information would be permitted to move over the cloud.

E. Features of the cloud computing

The cloud is now hosting wide range of large scale and small scale applications. Many organization or companies are now moving key applications from expensive internal data centers to cost effective and resourceful cloud solutions.

Scalability: When a user lunch website scalability defines a site or application's skill to use traditional solutions on demand. The site may scale up to available additional resources the system is experiencing high user demand and later may scale down recourse when the user demand turns down. Applications that run within the cloud are normally highly scalable. An applicant can manually add or remove resources or application can be configured to scale automatically.

Virtualizations: Virtualization is to use hardware or software to create the observation of something. Must server have their own CPU that is capable of running specific a specific operating system (OS), such as Windows, Linux, or Mac OS. By using special software, server can be shown as it has multiple CPUs and are running the same or different operating systems and the server CPU switches its processing power frequently among the various operating systems.

In the same way, desktop PCs typically run one operating system. Again, by using special virtualization software, a desktop PC/ laptop can be run simultaneously different operating systems. This provides an excellent platform for developer's application testers, and help desk support personal which support multiple operation systems. without having multiple systems on the desk, the user can use multiple operation systems in a single desktop PC.

F. Cloud Computing Simulators

During the study we compared various available cloud simulators, their properties and unique features. The comparison study along with the research group working on these tools are summarized in Table I.

III. Security Issues in Cloud

Here in this section we described several cloud computing security issues based on different service layer. The Fig. 3 shows the overlay architecture of security issues and trust requirement in a top-down service model [23]. Trust basically works in a top-down design, as every layer needs to trust the layer instantly beneath it, and obliges a security ensure at an operational, specialized, procedural and lawful level to empower secure correspondences. But the security is treated as individually in each service layer. Trust could be seen as a sequence from the end client to the application holder, who thusly believes the provider.

[1]http://docs.google.com
[2]http://www.salesforce.com/uk/crm/products.jsp
[3]http://code.google.com/appengine
[4]http://www.microsoft.com/windowsazure/
[5]http://aws.amazon.com/
[6]http://www.cs.standrews.ac.uk/stacc

TABLE I
COMPARISON OF CURRENTLY AVAILABLE CLOUD SIMULATORS

Simulator	Base Platform	Developer	Available	Language	GUI	Energy Model
CloudSim [30]	SimJava	University of Melbourne, Australia.	Open Source	Java	No	Yes
CloudAnalyst [31]	CloudSim	University of Melbourne, Australia.	Open Source	Java	Yes	Yes
iCanCloud [33]	SIMCAN	Universidad de Madrid, Spain.	Open Source	C++	Yes	No
NetworkCloudSim [32]	CloudSim	University of Melbourne, Australia.	Open Source	Java	No	Yes
EMUSIM [34]	CloudSim, AEF	University of Melbourne, Australia.	Open Source	Java	No	Yes
GroudSim [35]	-	University of Innsbruck, Austria	Open Source	Java	Limited	No
MRCloudSim [36]	CloudSim	Seoul National University, South Korea	Not available	Java	No	Yes
DCSim [37]	-	University of Western Ontario, Canada.	Open Source	Java	No	No
SimIC [38]	SimJava	University of Derby, UK	Not available	Java	No	Rough
GreenCloud [39]	NS2	University of Luxembourg, Luxembourg	Open Source	C++, otcel	Limited	Yes
MDCsim [40]	CSIM	Pennsylvania State University, USA	Commercial	Java, C++	No	Rough
SPECI [41]	SimKit	University of Bristol, UK	Open Source	Java	-	Rough
MalStone [42]	-	University of Illinois, Chicago, USA	Open Source	Java, Python	-	Rough

A. Security issues in SaaS

In SaaS, the client needs to rely on upon the supplier for fitting efforts to establish safety. The supplier must do the work to keep numerous clients' from seeing one another's information. So it gets to be hard to the client to guarantee that right efforts to establish safety are set up furthermore hard to get confirmation that the application will be accessible when required [24]. Based on SaaS, client can substitute net program or software applications over old one. Hence, the center is not upon portability of uses, yet on safeguarding or upgrading the security usefulness gave by the legacy application and attaining effective information relocation [29].

The SaaS programming seller may have the application on its own private server farm or convey it on a cloud computing framework administration gave by an outsider supplier (e.g. Amazon, Google, etc.). The utilization of cloud computing coupled with the pay-as-you-go (develop) methodology helps the application administration supplier diminish the interest in foundation benefits and empowers it to focus on giving better administrations to clients. Over the past decade, computers have become widespread within enterprises while IT services and computing has become a commodity. Enterprises today view data and business processes (transactions, records, pricing information, etc.) themselves as strategic and guard them with access control and compliance policies. However, in the SaaS model, enterprise data is stored at the SaaS providers data center, along with the data of other enterprises. Moreover, if the SaaS provider is leveraging a public cloud computing service, the enterprise data might be stored along with the data of other unrelated SaaS applications. The cloud supplier may, also, imitate the information at numerous areas crosswise over nations for the reasons of keeping up high accessibility. Most enterprises are acquainted with the conventional on-reason model, where the information keeps on residing inside the endeavour limit, subject to their approaches. Therefore, there is a lot of inconvenience with the absence of control and information of how their information is put away and secured in the SaaS model. There are strong concerns about data breaches, application vulnerabilities and availability that can lead to financial and legal liabilities [25].

There are several highlights security issues in SaaS such as data security, network security, data locality, data integrity, data segregation, data access, authentication and authorization.

B. Security issues in PaaS

In PaaS, the administration supplier may give some control to the customer to manufacture applications on top of the stage. However any securities beneath the application level, for example, have and system interruption anticipation will at present be in the extent of the supplier and the supplier brings to the table solid affirmations that the information stays distant between applications. Paas is proposed to empower designers to assemble their own particular applications on top of the platform. As a result, it tends to be more extensible than SaaS, at the expense of customer-ready features. This exchange off stretches out to security gimmicks and abilities, where the implicit capacities are less finish, however there is more adaptability to layer on extra security [25].

Applications sufficiently perplexing to influence an Enterprise Service Bus(ESB) need to secure the ESB straightforwardly, leveraging a convention, for example, Web Service (WS) Security. The capability to portion ESBs is not accessible in PaaS situations. Measurements ought to be set up to survey the viability of the application security programs. Among the immediate application, security particular measurements accessible are defencelessness scores and patch scope. These measurements can show the quality of application coding. Consideration ought to be paid to how malignant on-screen characters respond to new cloud application architectures that the darkened application parts from their examination. Programmers are liable to the assault noticeable code, including but not constrained to code running in the client connection. They are prone to assault the foundation and perform extensive black box testing. The vulnerabilities of cloud are connected with the web applications as well as vulnerabilities connected with the machine-to-machine Service- Oriented Architecture (SOA) applications, which are progressively being conveyed in the cloud [25].

C. Security issues in IaaS

In IaaS, the developer has better control over the security the length of there should not any security gap in the virtualization

director. Likewise, however in principle virtual machines may have the capacity to address these issues yet in practice there are a lot of security issues [26]. The other element is the unwavering quality of the information that is put away inside the supplier's equipment. Because of the developing virtualization of "everything" in data society, holding a definitive control over information to the holder of information paying little respect to its physical area will turn into a subject of most extreme investment. To accomplish most extreme trust and security on a cloud asset, a few procedures would need to be connected [27]. The security obligations of both the supplier and the client incredible contrast between cloud administration models. Amazons Elastic Compute Cloud (EC2) (Amazon, 2010) IaaS offering, as a case, incorporates merchant obligation regarding security up to the hypervisor, importance they can just address security controls, for example, physical security, natural security, and virtualization security. The client, thus, is in charge of the security controls that identify with the IT framework including the OS, applications and information [29].

Based on the cloud deployment IaaS inclined to various security issues. Private cloud is more protected compared to a public cloud. The most important issue is to protect the physical infrastructure of data centers. It can be damage by any natural disaster or damage is acquired to the framework deliberately. Infrastructure doesnt mean the hardware where data is processed and stored, it also include the where it is getting transmitted. In cloud environment data transmitted from the source to destination through large number of third party. So there is huge possibility that information could be directed through an interloper's foundation [25]. Despite the fact that cloud construction modeling is an extemporized engineering, the underlying advances continue as before. As cloud services are available online, it builds over internet and securities in web are postured by the cloud. It provides client access resources over the internet whenever supplier dwells at distinctive area.

Regardless of the fact that gigantic measure of security is placed set up in the cloud, still the information is transmitted through the ordinary underlying Internet. So threaten on the Internet is leading to cloud threaten. But, in a cloud, the dangers are devastatingly high. Cloud frameworks still use ordinary conventions and efforts to establish safety that are utilized within the Internet yet the prerequisites are at a higher degree. A dynamic set of arrangements and conventions are obliged to help secure transmission of information inside the cloud. Encryption and secure conventions coddle the needs to a certain degree yet they are not connection situated. Concerns with respect to interruption of information by outer nonclients of the cloud through the web ought to additionally be considered. Measures should be set in place to make the cloud environment secure, private and isolated on the Internet to avoid cyber criminals attacking the cloud [25] [28].

IV. Open Research Challenges and Directions

A. Handling Uncertainties

It has been demonstrated that one of the difficulties in provisioning cloud assets is uncertainty [10] [11]. Resource uncertainty emerges from a number of issues including client location, content type, noxious exercises, heterogeneity, and so forth. At times, multimedia content delivery application may confront with disappointment of resources or it may experience the ill effects of absence of sufficient resources. Considering that bandwidth is one of the most important resources especially in multimedia applications, lack of bandwidth may lead to huge degradation in QoS. In multimedia Application the amount of required bandwidth is largely affected by three factors: 1) Media application bandwidth demand; 2) user's workload bandwidth demand; and 3) user's location and device type. These factors change rapidly and may result in bandwidth shortage at some points. For provisioning enough bandwidth predicting these factors is critical:

- Multimedia application network bandwidth demand: Predicting the size of approaching video frames relying upon the transient history of the previously observed frames.
- User's workload bandwidth demand: Predicting user's workload (number of people requesting video) given the history of previous requests.
- Multimedia application resource demand: Dynamically predicting and capturing the relationship between multimedia application Qos targets, current hardware equipment allotment and changes in client's workload patterns.

By predicting above factors, the cloud resource provisioner can allocate the appropriate amount of bandwidth. Some methods [12] [13] [14] [15] for bandwidth and resource demand prediction are proposed in isolation, but these methods do not consider all of the above factors as part of single prediction process. This project will focus on both these factors for an appropriate prediction of bandwidth. Moreover, in media applications clouds providers have to deliver media to users according to their SLA agreement with multimedia application providers. One of the important components of SLA is that media frames must be provided in the user device before specified deadlines to guarantee a constant display. For addressing this issue, cloud providers must deal with link delays between clients and cloud servers. An important factor that directly affects the delay is the location of the media servers. According to the distribution of users appropriate allocation of the servers, closer to the user, will result in lower delays. As the clouds provide possibility for allocating servers in different places, it is possible to address this issue by means of clouds more efficiently. This project will present methods for proper allocation of clouds regarding the location of users.

B. Handling dynamic variations in workload

An important benefit of hybrid architectures of cloud that has not been explored above, is their potential to handle peaks in workload. In particular, the local data-center could be provisioned with enough server ability to handle workloads,

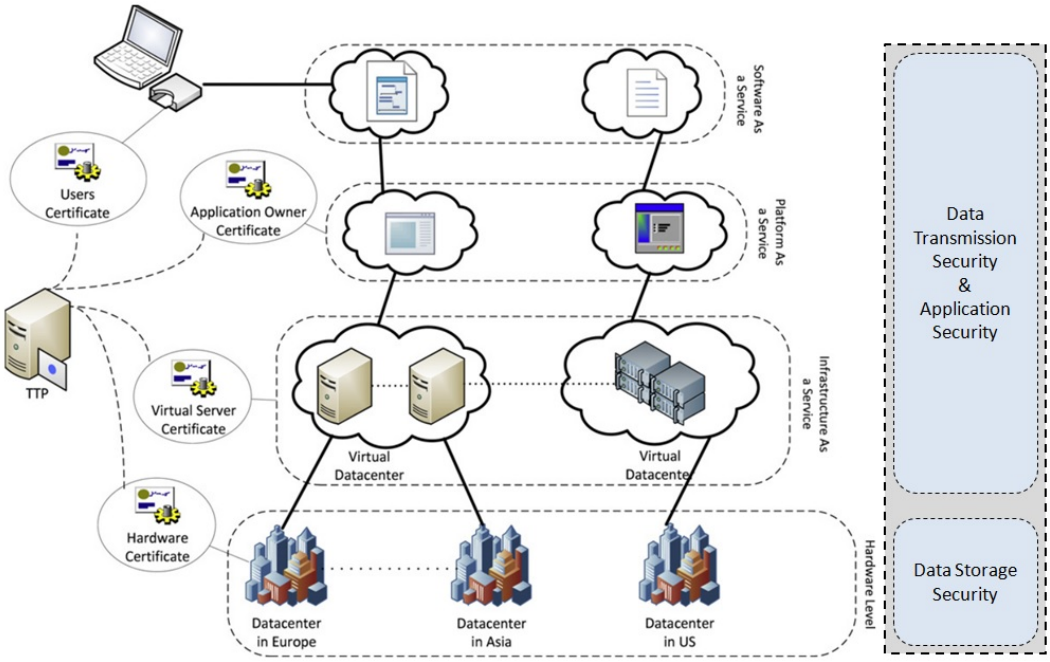

Fig. 3. Overlay architecture of security issues and trust requirement in a top-down service model.

while cloud assets could be invoked as required to manage peaks. The methodology could conceivably help in arranging formats that can manage dynamic workload varieties. One methodology is to utilize the model to focus the suitable configurations for a mixed bag of evaluated workloads, and build the final configuration on the expected probabilities of every workload. An alternate methodology is to utilize the model occasionally as workloads change over time, to figure out whether a change in placement is needed. More point by point examination of these issues can be conceded and an open opportunity to work on.

C. Optimisation of Virtual Network Topologies

In virtualised data centers VMs regularly communicate between one another, making virtual system topologies. However, because of VM migrations or no streamlined allocation, the communicating VMs may wind up facilitated on logically distant physical nodes giving expensive information exchange between one another. If the communicating VMs are dispensed to the hosts in diverse racks or enclosures, the network communication may include network switches that consume critical amount of power. To take out this information exchange overhead and minimize power utilization, it is important to observe the communication between VMs and spot them on the same or nearly placed nodes. To give compelling reallocations, the power utilization models can be developed of the network devices and assessment the expense of information exchange relying upon the traffic volume. As relocations consume extra energy and they have a negative effect on the execution, before launching the relocation, the reallocation controller needs to guarantee that the expense of migration does not surpass the profit.

D. Efficient of VMs Consolidation for Managing Heterogeneous Workloads

Cloud infrastructure services provide users the capacity to procurement virtual machines and assign any sort of uses on them. This prompts the way that distinctive sorts of uses (e.g., enterprise, scientific, and social network applications) might be allotted on one physical machine node. On the other hand, it is not evident how these applications can impact one another, as they might be information, network or compute intensive accordingly making variable or static load on the resources. The issue is to figure out what sort of uses might be designated to a single host that will give the most effective overall utilization of the resources. Current methodologies to energy proficient consolidation of VMs in data centers do not investigate the issue of consolidating diverse sorts of workload. These methodologies typically concentrate on one specific workload type or do not consider various types of uses assuming uniform workload. In contrast to the previous work, an intelligent consolidation of VMs with different workload types can be proposed. A compute intensive (scientific) application can be effectively combined with a web-application (file server) as the former mostly relies on CPU performance, whereas the latter utilizes disk storage and network bandwidth. In our opinion, which particular kind of applications can be effectively combined and what parameters influence the efficiency; and develop resource allocation algorithms for managing them can be investigated for a better approach. Moreover, this information might be applied to energy proficient resource management strategies in data centers to attain more ideal optimal allocation of resources and, accordingly, enhance usage of resources and decrease energy utilization.

For the resource suppliers, ideal distribution of VMs will bring about higher use of resources and, hence, diminished operational expenses. End-users will profit from diminished costs for the resource utilization.

E. Scientific Workflow Scheduling

Cloud computing offers tremendous opportunities to solve large-scale scientific problems in areas such as bioinformatics, astronomy, and physics. As cloud computing faced with various challenges like performance variations and failures. The performance variations affect the overall execution time of the workflow and failure affects the overall workflow execution and increase the execution time. The workflow scheduling on distributed systems has been widely studied over the years and is NP-hard by a reduction from the multiprocessor scheduling problem [17]. Current workflow scheduling on Clouds mostly focuses on homogeneous resources, and very fewer attempts have been made for the heterogeneous types of resources and one of the early attempts is made by Abrishami et al. [18]. The workflow management systems should handle performance variations and failures while scheduling workflows.

There are two main stages when planning the execution of a workflow in a cloud environment. In the resource provisioning phase i.e. first stage, the computing resources are selected and provisioned. In the second stage, a schedule is generated and each task is mapped onto the best-suited resource. The selection of the resources and mapping of the tasks is done so that different user defined quality of service (QoS) requirements are met [19]. Previous works in this area, especially those developed for Grids or Clusters, focused mostly on the scheduling phase. The reason behind this is that these environments provide a static pool of resources which are readily available to execute the tasks and whose configuration is known in advance. Since this is not the case in cloud environments, both problems need to be addressed and combined in order to produce an efficient execution plan. Hence, the future research efforts must take the dynamic provisioning and heterogeneity of unlimited computing resources in the account to develop techniques and framework that cater the heterogeneous computing environment.

F. Public Auditing

The popularity and rapid growth of cloud storage services to impart information to others has prompted an uncertainty in the integrity of data in cloud storage, as data stored in the cloud can easily be lost or undermined because of the inescapable hardware/software failures and human errors [20]. There numerous traditional approach for checking data correctness. The conventional approaches are able to successfully check the correctness of cloud data. However, the efficiency of using this traditional approach on cloud data is in doubt, as it is required to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures of the entire data [21]. The mechanism that efficiently perform integrity checking without downloading the entire data from the cloud is referred to as public auditing [22].

A public verifier or a third-party auditor provide expert integrity checking services. During public auditing on cloud information, the content of private information of an individual client is not disclosed to any public verifiers. Hence, new significant privacy issue, the leakage of identity privacy to public verifiers, is introduced. Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information to public verifiers. Developing techniques that can ensure the integrity of cloud storage, security and privacy remains a challenging research problem.

G. Data Availability

Availability refers to the property of a framework being available and usable upon interest by an authorized entity. System availability refers to carry on operations even when authorities mischief. The system must have the capability to carry on its operations even in the security violation. It also refers data, software, and hardware available to authorized users based on the demand. The cloud likewise ensures that data and data handling is accessible to customers upon interest. System availability incorporates a frameworks capacity to bear on operations actually when some authorities mischief i.e. it must continue operations even during security break. Cloud computing services show a substantial dependence on the resource frameworks and network accessibility at all times.

Comprehension and clearly documenting particular user requirements are imperative in planning a solution focusing at guaranteeing these requirements. Verifying identities many of which impart basic crucial security necessities and deciding particular requirements for information protection and data security could be a standout amongst the most perplexing components of IS outline. This multiuser dispersed environment proposes exceptional security challenges, reliant on the manager needs the level at which the user operates [23]. The major security issues in the cloud system are as follows [4]:

- Availability of information within participating systems;
- Maintain the integrity of information within the cloud, i.e. preventing the loss or modification of information due to unauthorized access or component failure. This is the major issue in public cloud;
- Provide control over access to services or their components to ensure that all are authorized;
- Clear separation of data and processes on the virtual level of the cloud, ensuring zero data leakage between different applications.
- To maintain the same level of security when adding or removing resources on the physical level.

Here we have line out seven different research directions in the current era of cloud computing research. Based on the features of cloud computing, we divided our research directions into different aspects such as scalability, virtualization, data management, cloud security and scientific applications. Those areas cover all the aspects of the cloud research and are helpful for a researcher to find out a unifying research direction. All the research opportunities describe the concept/working model in-depth and show the direction of future research aspects.

V. Conclusion

This paper discussed the emerging research issues that pursued the advance scientific features of cloud computing with layer wise classification of the cloud services, and highlighted the subsequent guidelines of research facing the both industry and academic community. This survey and future issues demonstrated that there are a few routes in which the cloud research group can gain from related groups. We have given an extensive outlook of current research issues cloud computing and available platform to simulate the research idea. We have exhibited scientific classification of issues found here, and the methodologies in which these issues have been handled, concentrating on an operational level, client level, service level and application level, security and context-awareness.

References

[1] Armbrust, Michael, et al. "A view of cloud computing." Communications of the ACM, 53(4), pp. 50-58, 2010.

[2] Sasikala, P. "Research challenges and potential green technological applications in cloud computing." International Journal of Cloud Computing, 2(1), pp. 1-19, 2013.

[3] Zissis, Dimitrios, Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation Computer Systems, 28(3), pp. 583-592, 2012.

[4] R. Sherman, Distributed systems security, Computers & Security 11 (1), 1992.

[5] Fernando, Niroshinie, Seng W. Loke, and Wenny Rahayu. "Mobile cloud computing: A survey." Future Generation Computer Systems, 29(1), pp. 84-106, 2013.

[6] Plummer, D.C., Bittman, T.J., Austin, T., Cearley, D.W. and Smith, D.M. "Cloud Computing: Defining and Describing an Emerging Phenomenon." Gartner, 2008.

[7] Staten, J. "Is Cloud Computing Ready for the Enterprise", 2008.

[8] Mell, P. and Grance, T. "The NIST Definition of Cloud Computing." 2009.

[9] Buyya, R., Yeo, C. and Venugopal, S. "Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities, HPCC, 10th Proceedings IEEE, pp. 5-13, 2008.

[10] Schad, Jrg, Jens Dittrich, and Jorge-Arnulfo Quian-Ruiz. "Runtime measurements in the cloud: observing, analyzing, and reducing variance." Proceedings of the VLDB Endowment, pp. 460-471, 2010.

[11] Iosup, Alexandru, Nezih Yigitbasi, and Dick Epema. "On the performance variability of production cloud services." CCGrid, 2011 11th IEEE/ACM International Symposium on, pp. 104-113. IEEE, 2011.

[12] Di Niu; Zimu Liu; Baochun Li; Shuqiao Zhao; , "Demand forecast and performance prediction in peer-assisted on-demand streaming systems," INFOCOM, Proceedings IEEE , pp. 421-425, 2011.

[13] Al-Tamimi, A.-K.; Jain, R.; So-In, C.;, "Dynamic resource allocation based on online traffic prediction for video streams," Internet Multimedia Services Architecture and Application(IMSAA), 2010 IEEE 4th International Conference on, pp. 1-6, 2010.

[14] Caron, E.; Desprez, F.; Muresan, A.; , "Forecasting for Grid and Cloud Computing On-Demand Resources Based on Pattern Matching," Cloud Computing Technology and Science (CloudCom), IEEE 2nd International Conference on , pp. 456-463, 2010.

[15] Kalyvianaki, Evangelia, Themistoklis Charalambous, and Steven Hand. "Self-adaptive and self-configured CPU resource provisioning for virtualized servers using Kalman filters." In Proceedings of the 6th international conference on Autonomic computing, ACM, pp. 117-126. 2009.

[16] Poola, Deepak, Saurabh Kumar Garg, Rajkumar Buyya, Yun Yang, Kotagiri Ramamohanarao. "Robust scheduling of scientific workflows with deadline and budget constraints in clouds." 28th IEEE Int. Conf. on Advanced Information Networking and Applications, pp. 1-8. 2014.

[17] T. Sousa, A. Silva, and A. Neves, Particle swarm based data mining algorithms for classification tasks, Parallel Comput., 30(5), pp. 767783, 2004.

[18] S. Abrishami, M. Naghibzadeh, and D.H.J. Epema. "Deadline-constrained workflow scheduling algorithms for infrastructure as a service clouds." Future Generation Computer Systems, 29(1), pp. 158-169, 2013.

[19] Rodriguez, M.A; Buyya, R., "Deadline Based Resource Provisioning and Scheduling Algorithm for Scientific Workflows on Clouds," Cloud Computing, IEEE T. on, 2(2), pp.222-235, 2014.

[20] K. Ren, C. Wang, and Q. Wang, Security Challenges for the Public Cloud, IEEE Internet Computing, 16(1), pp. 69-73, 2012.

[21] Boyang Wang; Baochun Li; Hui Li, "Oruta: privacy-preserving public auditing for shared data in the cloud," Cloud Computing, IEEE Transactions on , 2(1), pp.43-56, 2014.

[22] C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, Proc. IEEE INFOCOM, pp. 525-533, 2010.

[23] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation Computer Systems, 28(3), pp. 583-592, 2012.

[24] Choudhary, V. Software as a service: Implications for investment in software development. 40th Annual Hawaii International Conference on System Sciences, IEEE, 209a-209a, 2007.

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

[26] Gajek, S., et al. Breaking and fixing the inline approach. ACM workshop on Secure web services, ACM, 2007.

[27] Descher, M., et al. Retaining data control to the client in infrastructure clouds. International Conference on Availability, Reliability and Security, IEEE, pp. 9-16, 2009.

[28] Staten, James, et al. "Is cloud computing ready for the enterprise." Forrester Research, 2008.

[29] Seccombe A, et al. Security guidance for critical areas of focus in cloud computing. Cloud Security Alliance, 2(1), 2009.

[30] Calheiros, Rodrigo N., Rajiv Ranjan, Anton Beloglazov, Csar AF De Rose, and Rajkumar Buyya. "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms." Software: Practice and Experience, 41(1), pp. 23-50, 2011.

[31] B. Wickremasinghe, R. N. Calheiros, R. Buyya, CloudAnalyst: A CloudSim-based Visual Modeller for analysing Cloud Computing Environments and Applications, 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[32] Garg, S. K., & Buyya, R. NetworkCloudSim: modelling parallel applications in cloud simulations. In Utility and Cloud Computing (UCC), 4th IEEE International Conference on, pp. 105-113, 2011.

[33] A. Nunez, et al. iCanCloud: A Flexible and Scalable Cloud Infrastructure Simulator, Jr. of Grid Computing, 10(1), pp 185-209, 2012.

[34] R. N. Calheiros, M .A. S. Netto, C. A. F. De Rose, and R. Buyya, EMUSIM: an integrated emulation and simulation environment for modeling, evaluation, and validation of performance of cloud computing applications, Software-Practice and Experience, 43(5), pp. 595-612, 2012.

[35] S. Ostermann, K. Plankensteiner, R. Prodan, Th. Fahringer, GroudSim: An Event-Based Simulation Framework for Computational Grids and Clouds, Euro-Par 2010 Parallel Processing Workshops Lecture Notes in Computer Science, pp. 305-313, 2011.

[36] J Jung,H Kim, "MR-CloudSim: Designing and implementing MapReduce computing model on CloudSim, International Conference on ICT Convergence (ICTC), pp. 504-509, 2012.

[37] M. Tighe, G. Keller, M. Bauer, H .Lutfiyya, DCSim: A Data Centre Simulation Tool for Evaluating Dynamic Virtualized Resource Management, 8th international conference and 2012 workshop on systems virtualization management (svm) Network and service management (cnsm), pp. 385-392, 2012.

[38] S. Sotiriadis, N. Bessis, N. Antonopoulos, A. Anjum, SimIC: Designing a new Inter-Cloud Simulation platform for integrating largescale resource management, IEEE 27th International Conference on Advanced Information Networking and Applications, pp. 90-97, 2013.

[39] Kliazovich, Dzmitry, Pascal Bouvry, and Samee Ullah Khan. "GreenCloud: a packet-level simulator of energy-aware cloud computing data centers." The Journal of Supercomputing, 62(3), pp. 1263-1283, 2012.

[40] Lim, Seung-Hwan et al. "MDCSim: A multi-tier data center simulation, platform." In Cluster Computing and Workshops, 2009. CLUSTER'09. IEEE International Conference on, pp. 1-9. 2009.

[41] Sriram, Ilango. "SPECI, a simulation tool exploring cloud-scale data centres." In Cloud Computing, pp. 381-392. Springer, 2009.

[42] Bennett, Collin, et al. "Malstone: towards a benchmark for analytics on large data clouds." In Proceedings of the 16th ACM SIGKDD Int. Conf. on Knowledge discovery and data mining, pp. 145-152. 2010.