International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(3): 209-229
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

Cloud Computing Service Level Agreement Issues and Challenges: A Bibliographic Review

Sohail Razi Khan and Luis Borges Gouveia
IT Department, University of Fernando Pessoa, Porto, Portugal
35525@ufp.edu.pt, lmbg@ufp.edu.pt

ABSTRACT

Cloud Computing provides parallel computing and emerged as an efficient technology to meet the challenges of rapid growth of data. With the number of benefits come serious challenges related to poor Quality of Service (QoS) and standards offered by cloud providers. This is due to lack of uniformity in-terms of Service Level Agreements (SLAs) offered by various providers. The lack of uniformity is considered as a major barrier to the adoption of cloud technology. Due to confusion and absence of universal agreed SLAs, different quality of services is being provided. Currently there is no uniform performance model agreed by all stakeholders; which can provide performance criteria to measure, evaluate, and benchmark the level of services offered by various cloud providers in the industry. With the implementation of General Data Protection Regulation (GDPR) in the near future and demand from cloud users to have Green SLAs that provides better resource allocations mechanism, there will be serious implications for the cloud providers and its consumers due to lack of uniformity in SLAs and variable standards of service offered by various cloud providers. This paper is an attempt to conduct a detailed review in Service Level Agreement issues, discuss the SLA life cycle, the negotiation, and assurance challenges faced by cloud users while agreeing on SLA. The paper is an attempt to highlight problems and challenges due to lack of standards or uniformity in SLAs faced by the cloud industry. Until there is a uniform performance model that stipulates certain agreed metrics in the SLA which the entire industry follows there will be different QoS offered by cloud providers which will be serious challenge to the adoption of cloud technology.

KEYWORDS

CIA Triad (Confidentiality, Integrity, Availability), CSP (Cloud Service Provider), General Data Protection Regulation (GDPR), Service Level Agreement (SLA), QoS (Quality of Service).

1 INTRODUCTION

The cloud computing model significantly cut the IT infrastructure costs by providing on-demand access to vast IT resources that are available in the cloud. In order to meet the expectations of the cloud users, SLA is crucial as it defines a contract which details precisely the level of service that a cloud provider will offer. Before adopting a cloud computing technology, the contract detailing SLA need to be discussed and agreed by all the concern parties. There is a lack of uniformity in-terms of (QoS) and standards which is due to poor designed SLAs offered by various cloud providers. The cloud industry has failed so far to produce a universal agreed SLAs which is considered as a major barrier to the adoption of cloud technology. Due to confusion and absence of universal agreed SLAs, different level of services is being provided by cloud providers. The requirement is to produce a uniform performance SLA model agreed by all

stakeholders; which can provide performance criteria to measure, evaluate, and benchmark the level of services offered by various cloud providers in the industry.

The Cloud data centers consist of various components which can malfunction and affect the entire performance of the system e.g. failure of a physical server, network, or a virtual machine (VM) can degrade the performance [1] and lead to a violation of SLA that was signed between the cloud provider and users [2]. There is a debate that under these circumstances the cloud service provider should pay to the cloud customers for each violation [3]. The main purpose of SLAs is to provide concrete guarantees to the cloud customers to offer a good level of service which will ensure if anything goes wrong the provider will be responsible for any disruption. The problematic area is the QoS detailed on the SLA document, there is no mechanism to verify the level of service delivered. SLA consist of two main metrics which are uptime metric detailing the guarantees to the access of the services whereas second metric related to response time which states the quality of services offered. Different cloud providers offer different level of services, which can't be verified and there is no uniformity which creates confusion and poor QoS delivered to the cloud users. For cloud users it is impossible to verify the level of service offered and there should be a mechanism which allows the cloud users to verify each metrics and make the cloud providers accountable for the level of services offered [4]. With numerous benefits to cloud technology there are serious challenges related to the lack of uniformity in-terms of QoS and standards offered by various providers. This is due to poorly define SLAs or not meeting the set parameters of various SLAs which are resulting in poor QoS and considered as a major barrier in the adoption of the cloud computing technology. Different level of services provided and no uniform performance model; there is no performance criteria to measure, evaluate, and benchmark the level of services offered by these cloud providers and that is badly affecting the cloud adoption rate. With the implementation of General Data Protection Regulation (GDPR) in the near future there will be serious implications for the cloud providers and its consumers due to lack of uniformity and variable standards of service offered by various cloud providers [4]. Initially the paper discusses the SLA life cycle and various stages that are involved in the preparation of SLA life cycle management, followed by negotiation and assurance process that takes place before we agree on a final SLA. The next section of the paper, describes in-detail the issues and challenges due to lack of universal agreed SLA and how it is barrier in the adoption of cloud technology. The final section of paper discusses the implications of General Data Protection regulation and demand of Green SLA on the overall cloud industry and its overall consequence due to lack of universally agreed SLA.

2.0 LITERATURE REVIEW

2.1 SLA Life Cycle

SLA has multiple stages to develop and implement the life cycle management. The five stage are Service Development, Negotiation, and Marketing, Implementation and evaluation as highlighted in the following figure 1: Life cycle of service level agreement [5]. The main focus is that all SLA metrics should meet the agreed requirements and if the requirements are not met then violation decision has to be made based on the rule that is violated. The main purpose of cloud computing contracts is to define the SLA and ensure that all SLA conditions are met. These SLAs are around data protection legislation, security of data, data protection, location of data, licensing and retention of data. Whereas if there is no fixed or minimum set standards that can act as a benchmark then different quality of SLAs offered by the provider will not allow the cloud users to take full advantage of this technology.

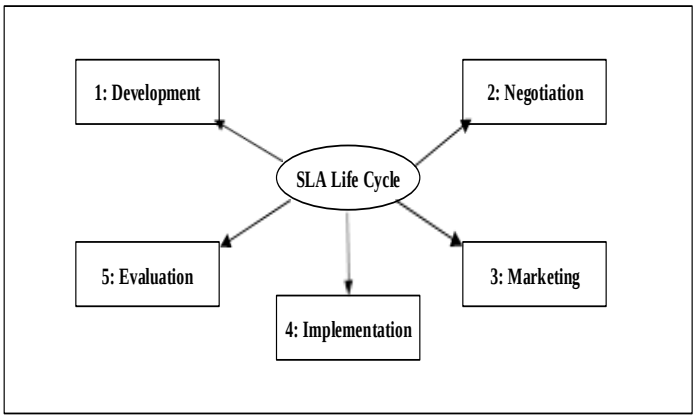

Figure 1: Life cycle of service level agreement [5]

Different models and frameworks were proposed that will enable the selection of the cloud providers. One of the major trends is Service-Oriented Architecture (SOA) in which the delivery of services is done by using the web service over the Internet [6]. The study helped to understand the management of resources and its impact on the service selection and optimization. Another proposed new approach for cloud service selection that is based in ranked voting of the existing cloud users [7]. The highest score will indicate the preferred cloud provider and also shows better data security and privacy. According to [8], QoS plays a key role in the service selection process especially for SaaS model. In CSMIC introduced the Service Measurement Index (SMI), which indicates various categories defined by various key entities. The model provides a Key Performance Indicators (KPI) for measuring and comparing the services. The study further elaborates that this selection technique is a complex process for ordinary users who have limited or no technical knowledge of cloud technologies. The framework was not able to provide a comprehensive suite of standards that meet all the key challenges faced by the cloud users who have limited knowledge and understanding about these complex issue while using or adopting the technology. The next section of the paper discusses the SLA assurances mechanism that incorporates the requirements of cloud users.

2.2 SLA Assurance

In order to improve the QoS and having uniformity in-terms of SLAs, [9] introduced the SLA assured brokering framework that incorporates the requirements of cloud users.

The research proposal ensures that SLA provided by the cloud provider to all its customers will be assured by having mechanism to measure the performance of the cloud applications. In the existing literature external cloud auditing measures the level of service provided by ranking according to the response time of the cloud providers. The author improves the model by ranking according to the quality of services which are provided by the cloud providers. Arpan Roy et al. [10] introduced the KIM software framework that introduces cloud controller that reduces the service failures that resulted due to the SLA violations. These SLA violations are utilization issues, availability, and response time violation in the SaaS data centers. The existing solution was to migrate so that they can overcome this failure. In the proposed work by Arpan Roy, the focus is on the service quality and issues related to performance level as stated on the SLA document. In order to improve the service quality, Sandpiper system for automated mitigation was proposed that will increase the response time of the physical machine and utilization in a virtualized data center due to workloads. The existing literature introduces the CloudScale system [11], that will act proactively to overcome any upcoming SLA violation and incorporates dynamic resource allocation in the addition to the migration of the work load. The proposed model uses Markov Chain based state space approach to predict and react to the upcoming SLA violations. The worked carried out by Salman [12], states that no cloud provider offer performance guarantees or allow customers to detect the SLA violation and there is a need of SLA assurance so that we can see the increase in the cloud adoption rate. In the next section of the paper details the negotiation approach that is adopted in order to agree the final SLA.

2.3 Negotiation Approach to SLA

The SLA should be agreed after a detailed negotiation process. This process should include the end user, data center and energy provider by considering the energy cost, energy resource and environment cost for providing services such as virtualization, integration, combination of data center, cooling system management and UPS which cater to the high energy demands in the data center [13]. The SLA framework should include the gradual changes of costs and client needs by introducing the automated negotiation process for SLA that includes a software mediator and providers that follows strategy based on factors such as time, market limitation, and tradeoff are considered [14]. The literature reinforces that the cloud resources are priced dynamically where the computation source is variable related to free capacity. The cost optimization process can be reviewed from the service provider view such as Random, Round-Robin, Greedy permutation and algorithm such as First-Fit used to evaluate work and compare them with implementation time. Ratio of successful cases and quality of solution [15]. In order to provide SLA, a trust model is presented that is based on trust management system and is called quality of service model because trust is designed based on the quality of service needs

[16]. The trust is calculated based on the four parameters such as accessibility, reliability, efficiency of returning data and data set that will be used to prepare SLA which is the combination of user quality of service needs and abilities of cloud source. The definition of SLA management depends on the negotiation process between cloud brokers and cloud providers and cloud brokers and cloud users and detailed effects of non-observing is mentioned [17]. The need of self-healing SLA can be useful such as HS-SLA method proposed for imposing a SLA, which is hierarchal and the mechanism includes SLA monitoring, detecting errors and reaction against that error and rapidly preventing against any errors [18]. This mechanism will prevent SLA errors as users will not be aware of any violations. The proposed scheme has experienced less violation as compared to other SLA strictures. In order to promote the negotiation process of SLA, safe negotiation system is proposed which is accessible for users in any time and by any device like a desktop, mobile which can reduce the overall maintenance costs [19]. These factors will be increase the efficiency process and the success through the negotiation process to formulate SLA will be carried out effectively. In the literature a proposed monitoring method is suggested that automatically monitors and controls the SLAs based on the policies of the users [20]. Different authors have proposed various SLA monitoring schemes which can monitor quality of service which is based on service description model and monitors SLA characteristics. The model such as QoSMONaaS [21], has the ability to produce queries to design patterns or sequence of patters which can detect violation in both pattern or find any violation that is happening currently. The model proposed in [22], is QoS-aware, and contains self-management ability which possesses the ability of cloud management and a quality of service factors that enables the cloud system to control and communicate system behavior. The following Table 1, shows a detailed comparison of various studies related to SLA.

Table 1: SLA comparison

Reference	Year	Goal Description	Implementation or Simulation	Implementation Environment	Workload or Application
9]	2012	Power Optimization			
10]	2013	1. Reduce cost of service receiver 2. Automatic negotiating	Implementation	Sigmoid & Heuristic Function	Real data
11]	2013	1)Reduce service provider cost 2) Dynamic pricing	Simulation	Testbed	Artificial data
12]	2013	Presenting Trust Model	Simulation	Cloudsim	Artificial data
13]	2012	1)Presenting Trust Model 2) SLA Management			
14]	2013	1)SLA automatic monitoring	Simulation	My SQL C#	Artificial data & empirical tests
15]	2014	1)Reduce service cost 2)Automatic negotiation 3)Security	Implementation	AmazoneS3	AmazoneS3 Storing Service
16]	2013	SLA automatic monitoring			
17]	2012	1)Present Trust Model 2)Detection before event occurrence 3) QoS monitoring	Implementation	Smart Meters Application	Smart Meters Application

3.0 ISSUES AND PROBLEMS DUE TO LACK OF SLA UNIFORMITY

3.1 Cloud Data Center Failures Issues

Due to lack of uniformity in-terms of SLAs there are serious challenges related to the failures of cloud data centers. These data centers can fail to operate due to any technical glitch. There is lack of clarity in-terms of SLAs, defining the consequences of data center failure. Various proposed work by Bilal & Ranjithprabhu *et*

al.[23], provides assurance of SLA compliance and introduced redundancy to eliminate the single point of failure in the cloud data center. In order to fulfil the SLAs the proposed work introduces data replication by using data mapping to prevent data losing in the cloud computing. The proposed work incorporates redundancy and replication to mitigate failures that may happen in the cloud data centers which host cloud provider services. This will ensure that there is no violation of SLAs and provides uniformity. This research highlights lack of clarity in-terms of SLAs related to the failure of cloud data center offered by various cloud providers.

3.2 E-Commerce Cloud-Loss of Control

The E-commerce cloud can be very useful to quickly build websites and reduce the cost of building or maintaining the websites. There are risks associated with the confidentiality of the data which is stored over cloud. There is a serious concern by end-users about the confidentiality of data that is stored over the cloud [24]. Serious issues have been raised in the capability of cloud computing to scale rapidly and store data remotely, where the services are shared among dynamic environment which can be problematic in-terms of data privacy assurance issues and maintaining the confidence of the potential users. Outsourcing these services can pose high risk to the cloud users as they lose control over their data couple with lack of clarity in-terms of SLA guarantees is a matter of concern for cloud users. The following Table 2, derives the main parameters for e-commerce cloud SLA framework.

Table 2: E-commerce cloud SLA framework

Parameters	Description	Citations
Availability	The uptime of the services for the user in specific time	[13] [20-21] [22] [23] [24] [25]
Scalability	Ability to increase and decrease the storage space	[13] [22] [25]
Portability	The services working on different devices or different platforms	[13] [22] [25]
Performance	The duration of time to respond on user's request	[13] [20] [21] [22] [24] [26]
Security	The security of user data and the safety of the environment in the cloud	[13] [21] [22]
Reliability	Services ability to operate over the time without failure	[13] [22] [25]
Usability	The ability of the service to be attractive, understandable, learnable, operable	[13] [22] [25]
Backup & Recovery	How the service store the image of user data and the ability to recover data in disaster	[13] [21] [20] [26]
Data Location	Availability zones in which the data are stored	[13]

3.3 Data Confidentiality and Privacy Concerns

The cloud technology enables businesses to store information in cloud, e-commerce businesses will have a very difficult time to supervise and monitor user's business sensitive information. Using the virtualization techniques, it becomes impossible to find the location of stored data [25]. Privacy is another major concern in the cloud computing where the design of the cloud infrastructure makes it difficult for cloud users where the current data is stored leading to privacy and protection issues. This is due to the transnational nature of cloud computing that has to face the national regulation privacy [26]. The existing cloud service level contracts and not taking sufficient attention on cloud users privacy and main cases have been reported of consumers poorly informed about the privacy issues [27]. The study carried by European Network and Information Security Agency [ENISA], tried to investigate the key issues related to cloud computing security issues. According to the survey conducted more than 70%, of the small and medium size enterprises are concerned in the following six criteria of security issues especially confidentiality issues. As per the following table 3, the main security issues facing the organization are as follows:-

Table 3: Security concerns by (ENISA)

Criteria	Very Important	Showstopper	Total
Confidentiality of Corporate data	30.9%	63.9%	94.5%
Privacy	43.9%	43.9%	87.8%
Availability of Service and/ or data	47.3%	40.0%	87.3%
Integrity of services and/or data	42.6%	44.4%	87.0%
Loss control of services and/or data	47.2%	28.3%	75.5%
Lack of liability of providers in case of security incidents	43.1%	29.4%	72.5%
Repudiation	47.9%	8.3%	56.2%

3.4 Application Delivery Chain Issues

The cloud based application are working due to a complex and extended delivery chain which involves the components that cross the geographical boundaries and extended across time zones [27]. The performance of the delivery chain and all components can directly affect the performance and user experiences. According to the research majority of service level agreement offered by the cloud providers are not taking in account the application delivery chain components. A failure in any of these applications in the application delivery chain can lead to major difficulties for cloud users to retrieve their data.

3.5 The Cost of Cloud Break Down

The failure of cloud service can happen as we experienced in April, 2011, Amazon EC2 faced 4 days of outages in the cloud services which affected millions of users. Various e-commerce companies faced serious financial and reputational damages but this event didn't violate Amazon service level agreement because

it was not clear in the terms and conditions stated in the SLA. The end-users blamed the e-commerce website for this but actually it was a failure at the part of the cloud provider but due to weak SLAs, it will not be held accountable for this. In the existing literature, some have proposed to maintain the reliability among cloud providers and consumers to include them in the negotiation process. The existing literature proposes [28], a mechanism to manage the SLA in a cloud environment by using the Web Service Level Agreement [WSLA], that will monitor and enforces SLA in a Service Oriented Architecture (SOA). The proposed framework provides a mechanism to manage the requirements of cloud consumers and enforces providers to follow SLAs based on the WSLA specifications that argue to adapt the Services-oriented-Architecture (SOA). The framework ensures the service quality and reliability standards are met. According to the literature, the problem with the framework is that doesn't completely support the whole SLA lifecycle. The next major issue with the framework is that the negotiation process is considered outside the framework [28], whereas IBM proposes a framework for SLA that is based around WSLA which incorporates negotiation process within the design of SLAs. In the next literature [29], proposed a framework for cloud SLA management named LoM2His, which is a sunset of FoSII *(*Foundations of Selfgoverning ICT Infrastructures) project[30]. In this proposed framework the low-level resources metrics map to the High-level SLA parameters. The model supports the monitoring and enforcement parts of the SLA lifecycle. In the existing literature [31-32], SLA attributes are different for various demands. The literature clearly mentions that due to the lack of standardization of SLA and no consistent framework is available to reference it becomes difficult for consumers to compare between the cloud services providers. It becomes a serious challenges for the cloud users to select a providers due to lack consistency in-terms of universal service level agreement. The next literature [33], introduces a conceptual platform of SLA in cloud computing that proposes a Reputation System for evaluating the reliability and trustworthiness of the provider. The framework proposes a SLA template pool in order to make the SLA negotiation process between cloud providers and cloud consumers more fair and transparent services. The framework allows the cloud provider to advertise their services and consumers can find and select the services which meet their demands. There are practical issues in advertising their services and cloud user selecting these services. The table 4 below concludes the existing SLA framework and their components.

Table 4: SLA framework components [33]

Framework & Authors	Components in SLA Lifecycle					
	Definition	Negotiation	Deployment	Monitoring	Management	Termination
Patel & Ranabahu (2009)			X	X	X	
V.C. Emeakaroha, I. Brandic & M. Maurer (2010)				X	X	
M. Alhamad, T. Dillon & E.Chang (2010)		X				
M. Wang, X. Wu, W.Zhang & F. Ding (2011)		X		X		
M. Torkashvan & H. Haghighi (2012)	X	X	X	X	X	X

There is a need of mechanism to measure the performance of SLA which will improve the overall quality of services offered by the provider [34]. According to the existing literature majority of the cloud providers only focuses on a small set of metrics such as availability, request completion rate and response rate. As reinforced by [35], a detailed study that breaks down the cloud SLA into easy and understandable metrics to compare SLAs in the cloud provider. The study tries to compare SLA of Amazon, Rackspace, Microsoft, Terremark vCloud Express and Stomon, and no provider was able to offer a performance guarantee for the services offered. This study also highlighted the fact that no provider has the structure to automatically credit the consumers for SLA violations. The study identifies the problem that unfulfilled expectations are due to the poor choice of parameters [36].

3.6 Security and Transparency Challenges

The security and transparency are considered as the main requirements for cloud service providers (CSPs). A Cloud SLA is a documented agreement between the CSP and the Customer that identifies Cloud services and service level objectives (SLOs), which are the targets for service levels that the CSP agrees to meet. If a SLO defined in the Cloud SLA is not met, the Cloud Customer may request a remedy (e.g., financial compensation). If the SLOs cannot be (quantitatively) evaluated, then it is not possible for Customers or CSPs to assess if the agreed SLA is being fulfilled. This is particularly critical in the case of secSLAs, but it is also an open challenge on how to define useful (and quantifiable) security SLOs? Due to lack of assurance and transparency coupled with security issues result in cloud customers not able to assess the security of the CSP for which they are paying. This raises two main questions which are how small or medium size business can assess whether CSP can fulfil their security requirements and the second issue is how CSP can provide security assurance to cloud users throughout the cloud service life cycle. The cloud user require a mechanism and tools that provide them with “good-enough” security in the cloud infrastructure [37]. Various stakeholders such as ENISA [38], ISO/IEC [39] and European Commission [40], have proposed various security parameters in Service-Level Agreement known as secSLA. The literature proposes security metrics by the introduction of Quantitative Policy Trees (QPT) [41], and Quantitative Hierarchical Process (QHP) [42] that obtains precise information regarding the security level using the Cloud secSLAs. According to the literature SLO metrics should contain quantitative and qualitative metrics where boundaries and margins should be set for CSPs. These are the limitation for CSPs to follows. The same security control framework has been proposed by ISO/IEC 27002 [43], the Cloud Security Alliance Matrix [44], and the National Institute of Standards and Technology SP 800-53 [45]. This mechanism provides an extra layer for security for the end user by

providing boundaries and margins as a guideline to the CSPs to abide by them.

3.7 CIA Triad Issues

Cloud Computing is an emerging market and its growing at an exponential rate. The adoption process of a cloud provider is a daunting tasks as it entails very complex details in-terms of data security and privacy issues that has to be considered by the potential cloud users [46]. The author explains further that the selection process is more complex then proposed multi-objective optimization, that overcomes some of the limitation in the selection of the cloud provider but the provision of Pareto front of optimal solutions creates the selection of the final solution more problematic as data security and privacy concerns are overwhelming. The author explains that for the potential cloud users' data security, data confidentiality, integrity, and availability are serious concerns as reinforced by the Figure1: Facet of Security. The particular research is focused only on the security solution rather than having a comprehensive approach to have universal standards for each parameter that are essential in the selection and evaluation of the Quality of Service (QoS) offered by any particular cloud provider.

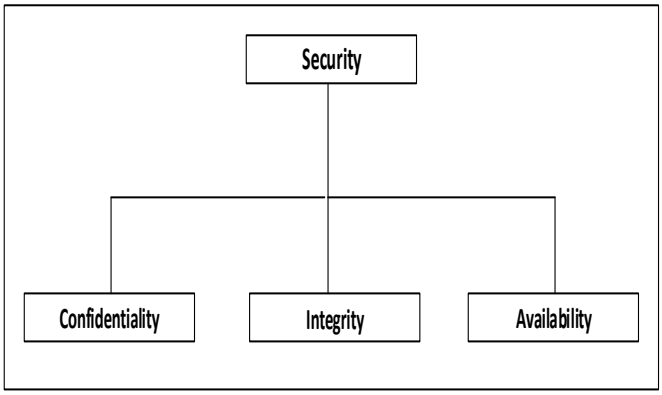

Figure 2: Facet of security issues [46]

In the existing literature there are proposed models such as [47], where the entire selection of the service is according to the consumer's perception and their experiences. The model proposed by [48] is an attempt to address the data security concern by introducing Third Party Auditors (TPA) mechanism for assurance and security of data. TPA will verify the integrity of the data and ensure that the message exchange are authentic. The research was not able to answer many other problems and concerns such as variable standards in availability, authentication, data protection laws and many other issues that cloud users are facing while planning to adopt or use the cloud technology. Many SLAs offered by various providers don't address serious challenges such as audit mechanism, data confidentiality and availability concerns of the cloud users.

The model proposes by [49], is based on few applications; as model lacks on weighting mechanism of cloud services that are linked to the cloud provider proposes a cloud ranking algorithm that revolves around a ranking algorithm based on functional parameters such as data security standards and privacy standards

but fails to incorporate the delivered services in their framework or set standards that will defines those delivered services across the industry. The model is based around consumers' experience, involves a third party to monitor and oversee the entire process but lacks in the performance measurements and evaluation framework which can address poor or variable standards of services offered by various providers. The next section will discuss Notorious Nine threats to cloud technology and how variable SLAs standards are aggravating the situation further.

3.8 The Notorious Nine: Cloud Computing Threats

The major security challenge faced by cloud computing is security and privacy of data. The concern related to security and privacy of data is raised due to the decrease in the rate of reliability and efficiency. Security in cloud computing has become the most important topic which needs urgent attention [50]. The literature highlights user authentication, access control issues, incident response mechanism, and variable set of SLAs standards as a serious challenges faced by the cloud based environment affecting both the service providers and end-users. The data security and privacy challenges are a major concern in the adoption of cloud technology. In the past many studies, researcher have tried to propose solution to improve security, privacy, efficiency and reliability of managing access and ensure authentication but still there are no uniform minimum standard of services agreed by the cloud industry. Due to variable quality of services and standards there are many cases reported of data breaches [51] and report publish by Cloud Security Alliance identifies lack of uniform consistent model that all cloud providers have to follow and held accountable as a major problem in the adoption of cloud computing technology.

Different studies have identified that data related to critical applications and sensitive in nature to be hosted over the cloud has always raised serious concerns as the data is continuously moved between the data center network and the client setup. The system is considered to be secure when we reduced all the threat to a minimum level that is acceptable to the organization. To provide better user authentication and access control some model are applying various solution such as Applying agent-based authentication system [52] and multi-factor authentication process [53] both these solutions can increase reliability of authentication process but fails to provide a comprehensive uniform model that can address serious challenges such as "The Notorious Nine: Cloud Computing Threats" as mentioned in the Table 5. Due to the absence of a uniform framework that provide minimum service level assurance these threats are a major barrier in the adoption and use of cloud technology.

Table 5: The Notorious Nine: cloud computing threats [50][51]

Threat	Description
Data Breaches	Release of protected data in an untrusted environment
Data Loss	Information is lost due to improper storage, transmission or processing
Account or Service Traffic Hijacking	Attack methods such as fraud and exploitation of service
Insecure APIs	Attack on code-signing keys used by web and cloud for identification
Denial of Service	Refusing user access to their data or application
Malicious Insider	Any insider misusing their authority to harm the cloud system
Abuse of Cloud Services	Using the cloud server and service for malicious activities
Insufficient Due Diligence	Risk due to incomplete understanding of the cloud infrastructu
Shared Technology	Attack due to multi-tenant architecture, re-deployable platform and shared resources

The non-functional requirements such as availability, confidentiality, integrity, scalability, response time, reliability, and monitoring and response mechanism are crucial to the cloud consumers to ensure better quality of service. The availability is the probability that the cloud infrastructure or service are up and running in the specific time of utilities of the service provided for in the SLA [54]. The other non-functional requirement is scalability; the cloud provider should facilitate the specific resources for ease of scaling up and down that will maximize revenue and cloud providers are able to optimize resource effectively. There is limitation in the existing work as there is no set standards or framework that are required for non-functional requirements that states the consequences if the cloud provider is not able to offer services up to an acceptable level. Also due to the absence of the framework some of the cloud providers are not offering an acceptable level of service and also to be held accountable according to a framework that is agreed by all the cloud providers in the industry.

Data availability and timely access to the cloud data is another serious security challenges for the cloud providers and users. The availability of the cloud service is becoming a serious challenge as cloud services are disrupted and the best example is Amazon cloud services in year 2011 got affected resulting in no service for various website such as Reddit, Foursquare and [55]. Services hosted on SaaS application provider are required to ensure effective services around the clock which means infrastructural changes to add scalability and high availability and resiliency in the hardware/software failure to protect against the denial of service attacks and appropriate business continuity and disaster recovery plan [56]. This can play a vital role by ensuring the safety of the data and maintaining a minimal downtime for any enterprise. In the case of Amazon, Amazon Web Services (AWS), to protect against these threats are using various mitigation techniques such as synchronous cookies, connection limiting, extra internal bandwidth and world class infrastructure but these procedure and standards are different for each provider as there is no benchmark framework that all providers are following to provider better QoS.

The confidentiality and information security is another concern of the existing and the potential cloud users. There are serious questions raised about the intentional or unintentional unauthorized disclosure of information. The data can be stored remotely it is accessed while using

internet connection [57]. The entire user's data can be stored at the same platform as other user's data which can lead to serious concern on data confidentiality and information security. As the data is stored outside the enterprise boundary, the SaaS vendor must adopt additional layers of security to protect and prevent any breach of data. The cloud vendors such as Amazon (EC2), administrators don't have access to customer instances and can't log into the guest OS. Administrator with business needs are required to use individual cryptographically strong secure shell to gain access. All accessed are logged and audited routinely. In terms of audit it's not clear whether a third party is allowed to carry out the audit and what procedures are followed. The data owner will not have a physical access to the data and traditional cryptographic primitives for the purpose of data security protection can't be directly adopted [58]. In this scenario, there is a need of third-party auditor (TPA), which provides efficiency, transparency and fairness in performing the required audit and closes the gap between the cloud provider and users. This mechanism provides realistic security solution where cloud users achieve majority of the cloud benefits at a very minor cost, the auditing of TPA is required. Currently this is a not a required standard and there is a legitimate concern for the security of data and confidentiality raised by the cloud users. As cloud provides a model that is based on multi-tenancy to reduce cost and improve the efficiency to host multi-users data in the same platform [59]. In these circumstances the data that belongs to different users will reside at the same storage location. This environment can lead to intrusion of data from one user to another by exploiting vulnerabilities at the application level or by infecting the code at the SaaS system [60]. There needs to be a mechanism that can define a clear boundary not at the physical level but at the application level to stop any intrusion. There is a need to have compatible solution that segregate data from the users and this solution followed by all the providers across the industry. Currently there is no uniform standard to ensure that data segregation doesn't take place and different providers provide different solution to this problem. The standards vary while making storing backups as well. For example in the case of Amazon the data at rest in S3 is not encrypted by default. The cloud users has to encrypt the entire data and define a backup strategy so that it can't be accessed by the unauthorized person and maintain confidentiality, integrity and availability. Data security, privacy, integrity and availability challenges have to be addressed so that more users can adopt cloud computing technology and feel comfortable while hosting their data on the third party servers. The next section of the paper discusses the implication of General Data Protection Regulation on the cloud industry and how lack of uniformity in-terms of SLAs will have serious consequences for cloud providers with the implementation of this new law.

4. IMPLICATION OF GENERAL DATA PROTECTION REGULATION

In order to protect and provide privacy to the data the new privacy framework has been recently initiated known as GDPR (General Data Protection Regulation), which provides a new policy to deal with the challenges of privacy of the data in the information society according to EU Parliament Commission report "Unleashing the Potential of Cloud Computing in Europe" published in 2016. The regulation (EU) 2016/679, provides protection to process the personal data and provides safeguards to the movement of such data within EU members. If GDPR regulation doesn't explicitly states about cloud computing, about the regulation is designed with cloud computing as a central focus of attention. According to the report publish by the commission, the law will be enforced in 2018, so the cloud providers should place systems to be prepared for the new rules and avoid any major issues in-terms of data security and privacy breaches as there will be serious implications for cloud providers with the implementation of GDPR law. In order to meet these new challenges and provide better security for cloud users the authentication and authorization need to be enhanced to provide a safe cloud environment. Forensic tasks is very difficult since the investigators are not able to access system hardware physically [61]. The resource location is a major concern for the end-users as most of the users don't know exactly where the resources for such services are located. This can lead to serious dispute that can happen which is not in control to the cloud providers. To save cost large amount of cloud providers are storing data across the world where data protection and privacy safeguards are not considered as rigors and comprehensive as compared to EU. This is a serious risk to the security and privacy of data as according to the data compliance and privacy laws states that locality of data has an importance for each enterprise. The European Union issued a Directive 95/46/EC that prohibits transfer of personal data to countries which do not ensure the adequate level of protection of data. There are many examples such as Dropbox users have agreed in the "Terms of Services" which grants the provider the right to disclose the personal users' information with the compliance to law enforcement request [62]. This raises serious privacy risk to the user data which needs to be addressed or it will have serious implications of cloud industry with the implementation of General Data Protection Regulation. The existing SLAs offered by the cloud providers are not adaptable to the changes that will effect according to the new regulation. There is a need for a uniform SLA model or a framework that can cater to the needs of GDPR and provide security and privacy to the cloud user's data and provide protection to cloud providers against any litigation.

5. GREEN ENERGY SLA

With the large usage of cloud computing services the question is that how green are these

services. The demand for green services have grown due to social awareness, the desire to provide green services and establish Green SLAs is crucial for cloud infrastructure providers. The challenge for cloud provider is to manage Green SLAs with their customers while satisfying their business objectives such as maximizing profits by lowering expenditure for green energy. In the existing literature the paper presents a scheme for green energy management in the presence of explicit and implicit integration of renewable energy in the data center. The literature proposes the concept of virtualization of green energy to address the uncertainty of green energy availability. The literature extends the Cloud Service Level Agreement (CSLA) to support Green SLA by introducing two new threshold parameters to offer SLA that meets the environment and green SLA requirements. The literature introduces greenSLA algorithm that introduces a concept of virtualization of green energy to provide per interval specific Green SLA. In contrast, Power-driven approach implies, shifting or scheduling the deferrable workloads to the time period when the price of electricity is lower or migrating workloads to the different region (data center) where the electricity price is cheaper than the origin with respecting the deadline. On the contrary, Green power-driven SLA can be realized as: end-users or SaaS providers shift their workloads in a renewable/green energy powered data center having an agreement with IaaS provider that some portion of their workload should run in a greener environment. Existing literature does not provide a clear idea about the advantages and disadvantages of different integration option of renewable energy sources in data centers. Although some research [63], [64], [65], [66] have explored the opportunity of integrating renewable sources in data center, but lacks the explanation of how SLA should be established between IaaS and SaaS providers based on the green energy availability.

To address this problem, the literature proposes a green power driven SLA framework established between SaaS and IaaS provider stating that, IaaS provider provides infrastructure with proportional e.g., 30 percent green energy availability. For instance, IaaS provider will have a formal contract with SaaS provider to provide green infrastructure based on a business model. In the following figure, SLAS_I contract used for showing two SLO of this layer, namely availability of physical resource and availability of green resource. Point to be noted that, a substantial amount of research [67], [68], [69], [70], [71], [72] has been already done both in industry and academia about efficient dynamic consolidation of PM, migration of VM and scalability issues in Cloud infrastructure. In position to these existing research, the work can be seen as complementary to their research since reducing energy consumption in infrastructure level and associating green sources can reduce carbon footprint in data center from the global point of view. The literature argues that Green SLA should be established by taking into account the presence of green energy rather just

reducing the energy consumption in the infrastructure level. The existing SLAs offered by the cloud providers are not adaptable to the changes that will effect due to Green SLAs requirements by the cloud users. There is a need for a uniform SLA model or a framework that can cater to the needs of Green SLAs.

6. RESOURCE ALLOCATION SLA

In the existing literature, SLA related to resource allocation is carried out based ion the cost factor. According to the literature [73], the main focus was to reduce the cost using cost effective genetic algorithm (CEGA) resulting in improved VM performance and reduce delay in the acquisition process. The literature [74], clearly mentions a framework that allows parallel processing which gives fast computation and resource availability to run lot more jobs in the single node as well through the entire machine. The framework will provide mechanism for mapping with reduced cost. For resource allocation there are major factors related to the time based RAM. The resource allocation [75], is the course of action offering the resources in at an accurate level based upon the workload associated. The resource mapping is done in a timely manner. In order to support dynamic adaption the framework [76], proposes a MIMO-Multi Input-Multi-Output feedback algorithm. The algorithm provides adaptive learning process and adapt the parameters to optimal resource allocations within the time constraints it faces. The literature also discuss the bargaining based approach [77], where cooperation based resource bargaining game involves the Service User and Service provider. The structure of algorithm works by taking initiating the bargaining steps by job submission followed by job execution that are described as cost, energy consumption and resources utilization. The literature has proposed various other approaches such as compromised cost and times based approach [78], where they pay based on the use of a particular feature. The feature reduces the cost by generating the execution time graph as compared to cost for the job that is executed currently. Then the user need to select the negotiation in-terms of cost and execution. The following table shows the study of Cost, Time, Bargaining and Cost & Time based RAM methods and the relationship between them.

Table 6: Resource allocation policies [78][79]

Cost	Time	Policy
Minimum	Minimum	Compromised Cost-Time Based
Maximum	Minimum	Time Based
Minimum	Maximum	Cost Based
Cost Agreement	Time Agreement	Bargaining Based

The next approach for resource allocation work around QoS metrics proposed [79], which is considered as a trustworthy resource sharing for cloud computing. The proposed work is uses harmony method which incorporates the resources and reputation management system and price assisted resource reputation control mechanism. The literature address Multi-faceted Resources/ Reputation Management, Multi QoS Oriented Resources Selection, Price Assisted

Resource/ Reputation Management. The approach will enable the most efficient service provider to the cloud users and calculate the reputation of each service node. The following table details the list of QoS Metrics and its purposes.

Table 7: QoS matrices and their purposes [79]

List of QoS Metrics	Purpose of Consideration
Response Time	To measure the ability of job processing ability of the CSP
Total Service Cost	To choose best and affordable service provider
Security of the Service	To ensure the security of the data processed on the cloud
Reputation	To choose the best service provider in oligopoly market within the budget cost of the user
Reliability	firmness of the service policies

The resource allocation research work is based on SLA developed in [80] that proposes a mathematical model to collect the tradeoff between minimizing a data center's energy cost versus maximizing the revenue it generates from the Internet services. Various factors are considered such as time, security, reputation, energy, and reliability in designing the resource allocation algorithm [81]. The cost resource allocation strategy tries to reduce the cost by using cost reduced genetic algorithm. The algorithm uses Time adapt resource allocation

7. CONCLUSION

The cloud industry is currently facing some serious challenges related to the lack of uniformity in-terms of Quality of Service (QoS) and standards due to poor designed and inconsistent Service Level Agreements (SLAs) offered by various cloud providers, which is considered as a major barrier to the adoption of cloud technology. Due to lack of uniformity and consistency in-terms of SLAs, different quality of service is being provided by various cloud providers. The situation becomes even graver due to the absence of any uniform performance model; which can provide performance criteria to measure, evaluate, and benchmark the level of services offered by these cloud providers. The challenges of agreeing on a universal SLA is one of the main factor that is affecting the cloud adoption rate. The paper provided a detailed bibliographic review of various challenges and problems due to the lack of uniformity in-terms of SLAS. In the near future the challenges for cloud industry will become more daunting with the implementation of General Data Protection Regulation (GDPR) and demand from cloud users to have Green SLAs with better resource allocation procedures will have serious implications for the cloud providers. For the future work a universal agreed SLA, which provides metrics to resolve the challenges and problems faced by the cloud user is crucial to improve the cloud technology adoption rate.

REFERENCES

[1] M. Ali and M. H.Miraz, "Cloud computing applications," *Internaional Conference on Cloud Compuing and eGovernance*, June. 2013.

[2] P. Patel, A. Ranabahu, and A. Sheth, "Service level agreement in cloud computing," *The Ohio Center of Excellence in Knowledge-Enabled Computing (Kno.e.sis)*, July. 2009.

[3] T. Wood, P. Shenoy, A. Venkataramani, and M. Yousif, "Sandpiper:Black-box and gray-box resource management for virtual machines," *Computer Networks*, vol. 53, no. 17, p. 2923:2938, Dec. 2009.

[4] S. S. Wagle, "SLA assured brokering (SAB) and CSP certification in cloud computing," *IEEE/ACM 7th International Conference on Utility and Cloud Computing*, Dec.2014.

[5] Columbus, L. (Dec. 7, 2017). Forbes, Roundup of cloud computing forecasts and market estimates, [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates 2017/&refURL=https://www.google.ae/&referrer=https://www.google.ae/ [Accessed 07/12/2017]

[6] Arjun, R and Vinay, A. "A short review on data security & data privacy issues in cloud computing. IEEE Transaction on Dependable and Secure Computing, Volume:6, pp.238-248, Sept. 2016

[7] Eisa, M., Younas, M., Basu,K., and Zhu, H. "Trends and directions in cloud service selection", IEEE Symposium on Service-Oriented System Engineering, March-April pp 1-25, May. 2016

[8] Gadia, S., (Aug.4, 2016). Forbes. "How to manage 5 key risks in cloud computing, KPMG Voice, [Online] https://www.forbes.com/sites/kpmg/2016/09/15/how-to-manage-5-key-risks-in-cloud-computing/#2c0368057542 [Access Date 15.05.2017]

[9] A. Roy, R. Ganesan, and S. Sarkar, "Keep it moving: Proactive workload management for reducing SLA violations in large scale SaaS clouds," *IEEE 24th International Symposium on Software Reliability Engineering (ISSRE)*, Sept. 2013.

[10] Z. Shen, S. Subbiah, X. Gu, and J. Wilkes, "Cloudscale: elastic resource scaling for multi-tenant cloud systems," *in Proc. SOCC. ACM*, p. 5:19, Dec. 2011.

[11] Salman A. Baset, "Cloud SLAs: Present and future," *IBM Research, ACM SIGOPS Operating Systems Review*, vol. 46 Issue 2, pp. 57–66, July 2012.

[12] S. Klingert, A. Berl, M. Beck, R. Serban, and M. Girolamo, "Sustainable energy management in data centers through collaboration. Energy Efficient Data Centers," Springer Berlin Heidelberg, vol. 7396, pp. 13-24, Apr. 2012.

[13] L. Wu, S. Kumar, and R. Buyya, "Automated SLA negotiation framework for cloud computing," 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 235-244, Dec. 2013.

[14] W. Li, P. Svard, J. Tordsson, and E. Elmroth, "Cost-optimal cloud service placement under dynamic pricing schemes," 9th IEEE/ACM International Conference on Utility and Cloud Computing, pp. 187-194, Dec. 2015.

[15] P. Manuel "A trust model of cloud computing based on quality of service," Springer US, New York, Print ISSN. 0254-5330, May 2014.

[16] P. Khanna, and B. Babu, "Cloud computing broking service: A trust framework," The Third International Conference on Cloud Computing, Grids, and Virtualization, pp. 206-212, March. 2012.

[17] A. Mosallanejad, R. RAtan, R. Abdullah, A. Murad, and T. Javdani, "HS- SLA: A hierarchical self- healing SLA model for cloud computing," pp. 1-11, June.2016.

[18] A. More, S. Vij, and D. Mukhopadhyay, "Agent based negotiation using cloud - an approach in E-commerce," 48th Annual Convention of Computer Society of India-Vol 1 Advances intelligent Systems and Computing, vol. 248, pp. 489-496, June 2017.

[19] K. Clark, M. Warnier, F. Brazier, "Self-adaptive service level agreement monitoring in cloud environments," Journal Multi agent and Grid Systems, May 2016.

[20] G. Cicotti, L. Coppolino, R. Cristaldi, S. D'Antonio, and L. Romano, "QoS monitoring in a cloud services environment: the SRT-15 Approach," Parallel Processing Workshops Lecture Notes in ComputerScience, Springer Berlin Heidelberg, vol. 7155, pp. 15-24, June. 2012.

[21] I. Ayadi, N. Simoni, G. Diaz, "Qos-aware component for cloud computing," 9th International Conference on Autonomous System (ICAS), pp. 14-20, Dec. 2013.

[22] L. Wu, S. kumar, and R. Buyya, "SLA-based Resource Allocation for Software as a Service Provider (SaaS) in Cloud Computing Environments," 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 195-204, June. 2015

[23]P. Patel, *et al.*, "Service level agreement in cloud computing,".Dec. 2010.

[24] M. Torkashvan and H. Haghighi, "CSLAM: A framework for cloud service level agreement management based on WSLA," in *Telecommunications (IST), 2012 Sixth International Symposium on*, pp. 577-585, Dec. 2012.

[25] V. C. Emeakaroha, *et al.*, "Low level metrics to high level SLAs - LoM2HiS framework: Bridging the gap between monitored metrics and SLA parameters in cloud environments," in *High Performance Computing and Simulation (HPCS), 2010 International Conference on High Performance Computing*, pp. 48-54, June. 2010.

[26] L.C. Baldor. (Aug 11, 2016). *Foundation of Self-governing ICT Infrastructures(FoSII)* [Online] Available: http://www.infosys.tuwien.ac.at/linksites/FOSII/index.html

[27] M. Alhamad, *et al.*, "Conceptual SLA framework for cloud computing," in *Digital Ecosystems and*

Technologies (DEST), 2010 4th IEEE International Conference on, 2010, pp. 606-610, Sept, 2010.

[28] M. Rady, "Parameters for service level agreements generation in cloud computing," in *Advances in Conceptual Modeling*. vol. 7518, S. Castano, *et al.*, Eds., ed: Springer Berlin Heidelberg, pp. 13-22, Sept 2015.

[29] M. Wang, *et al.*, "A conceptual platform of SLA in cloud computing," in *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, 2011, pp. 1131-1135 Dec, 2011.

[30] L. Greiner and L. G. Pau. (March, 2009). *SLA Definitions and Solutions*. [Online] Available:http://www.cio.com/article/128900/SLA_Definitions_and_Solutions?page=1#what

[31] F. Zhu, *et al.*, "A service level agreement framework of cloud computing based on the cloud bank model, " in *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on*, pp. 255-259, Dec, 2015,.

[32] J. Bouman, *et al.*, "Specification of service level agreements, clarifying concepts on the basis of practical research," in *Software Technology and Engineering Practice, 1999. STEP'99. Proceedings*, pp. 169-178. March. 1999,

[33] A. Paschke and E. Schnappinger-Gerull, "A Categorization scheme for SLA metrics," *Service Oriented Electronic Commerce*, vol. 80, pp. 25-40, Dec. 2011.

[34] S. A. Baset, "Cloud SLAs: present and future," *ACM SIGOPS Operating Systems Review*, vol. 46, pp. 57-66, March 2016.

[35] C. A. Ben Pring, William Maurer, Alexa Bona, "Best practices for service-level agreements for software as a service," Gartner Stamford G00208699, March 2010.

[36] M. Rady, "Parameters for service level agreements generation in cloud computing," in *Advances in Conceptual Modeling*, ed: Springer, pp. 13-22, March 2016.

[37] N. Ghosh and S. K. Ghosh, "An approach to identify and monitor SLA parameters for storage-as-a-service cloud delivery model," in *Globecom Workshops (GC Wkshps), 2012 IEEE*, , pp. 724-729, Dec 2016.

[38] A. Keller and H. Ludwig, "The WSLA framework: specifying and monitoring service level agreements for web services," *Journal of Network and Systems Management*, vol. 11, pp. 57-81, July, 2015.

[39] "Guidelines on information security controls for the use of cloud computing services based on ISOIEC 27002," International Organization for Standardization, ISOIEC 27002, Dec, 2014.

[40] Cloud Security Alliance. Cloud controls matrix v3. [Online]. Available: https://cloudsecurityalliance.org/research/ccm/, July. 2015.

[41] NIST "Security and privacy controls for federal information systems and organizations," National Institute of Standards and Technology, NIST 800-53v4, March. 2014.

[42] R. Sandhu, "Good-enough security: Toward a pragmatic business driven discipline," IEEE Internet Computer., vol. 7, no. 1, pp. 66–68, Jan. 2003.

[43] "Survey and analysis of security parameters in cloud SLAs across the European public sector," European Network and Information Security Agency, 2011-12-19, July. June 2014.

[44] "Information technology-cloud computing? Service level agreement (SLA) framework and terminology (Draft)," International Organization for Standardization, ISO/IEC 19086, June 2016.

[45] "Cloud service level agreement standardization guidelines, "European Commission, C-SIG SLA, Dec 2015.

[46] V. Stantchev and G. Tamm, "Addressing non-functional properties of services in IT service management," in Non-Functional Properties in Service Oriented Architecture: Requirements, Models and Methods". Hershey, PA, USA: IGI Global, pp. 324_334, Dec 2016.

[47] Mell, P and Grance, T. (2012). The NIST definition of cloud computing recommendations of the national institute of standards and technology special publication 800-145. Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, [Accessed: 18/03/2017].

[48] Mell, P and Grance, T. (2011). "NIST Definition of cloud computing", Special Publication 800-145.

[49] Baranwal, G. and Vidyarthi, D. P. "A cloud service selection model using improved ranked voting method', Concurrency and Computation: Practice and Experience", Journal of Systems and Software, Volume 108, Pages 60–76, Dec 2016.

[50] Press Release, Eur. Comm'n, Progress on EU data protection reform now irreversible following European Parliament vote (on file with author); Eur. Parl., *Q&A on EU data protection reform*, http://www.europarl.europa.eu/news/de/news-room/content/20130502BKG07917/html/QA-on-EU-data-protectionreform [Access Date 20.05.2017]

[51] Radha. K, Babu, Shaik and Rao. "A relative study on service level agreements in cloud computing", *Proceeding of 2015 Global Conference in Communication Technologies (GCCT), Volume No 3, pp.138-152*, June. 2015

[52] Baranwal, G. and Vidyarthi, D. P.”A cloud service selection model using improved ranked voting method”, Concurrency and Computation: Practice and Experience, Journal of Systems and Software, Volume 108, Pages 24-60, Dec 2016.

[53] Gutte, S. and Deshpande, P. , “Privacy preserving technique to secure cloud” Ipgcon-2015 Fourth Post Graduate Confernece, IJSWS 15-153, June 2015.

[54] Garg, S.K.; Versteeg, S. and Buyya, R.,"SMICloud: A framework for comparing and ranking cloud services," in Utility and Cloud Computing (UCC), Fourth IEEE International Conference on, vol., no., pp.210-218, 5-8. doi: 10.1109/UCC.2011.36, June 2011.

[55] Zheng, Z; Wu, X; Zhang, Y; Lyu, M.R; Wang, J. "QoS ranking prediction for cloud services," In Parallel and Distributed Systems, IEEE Transactions on , vol.24, no.6, pp.1213-1222, doi: 10.1109/TPDS.285, June 2016.

[56] Joshi, P and Pearce, C, "Automating cloud service level agreements using semantic technologies", Proc. of the 2015 IEEE International Conference on Cloud Engineering (IC2E), 9-13 March 2015, Tempe, AZ, USA, pp.416-421, Jan 2015.

[57] Cao, N. Wang, C. Li, M. Ren, K. and Lou, W. “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, March. 2014.

[58] Burkon and Lukas, “Quality of service attributes for software as a service”, Journal of System Integration, vol. 4 issue 3, pp. 38, Dec. 2015.

[59] Delettre, C. Boudaoud, K. and M. Riveill, “Cloud computing, security and data concealment,” in Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC ’11), pp. 424–431, Kerkyra, Greece, Dec, 20116

[60] Guzek, M; Gniewek, P; Bouvry, J; Musial, and Blazewicz, J, “Cloud brokering: Current practices and upcoming challenges,” *IEEE Cloud Computing*, vol. 2, no. 2, pp. 40–47 Mar. 2016.

[61] Cloud Security Alliance," [Online]. Available:https://cloudsecurityalliance.org/download/the-notorious-nine-cloudcomputing-top-threats-in-2013/ [Accessed 11.04.2017]

[62] Manvi, SS and Shyam, GK., “Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey”. Journal of Network and Computer Applications. 41, 424–440, March. 2017.

[63] A. Manzalini et al., “Towards 5G software-defined ecosystems technical challenges, business sustainability and policy issues,” IEEE SDN White Paper, retrieved July 2016 http://sdn.ieee.org/publications .

[64] F. Hu, “Security and privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations”, CRC Press, pp.281, Jan. 2016

[65] A. Nygren, B. Pfa, B. Lantz, et al., “The OpenFlow switch specification,” Version 1.4.0, Open Networking Foundation, Wire Protocol 0x05, ONF TS-012, October 2013.

[66] M. Betts, N. Davis, R. Dolin et al., “SDN Architecture,” Issue 1, Open Networking Foundation , ONF TR-502, June 2014.Syst., pp. 391–400, Aug. 2012,.

[67] Y. Kouki, F. Alvares, S. Dupont, and T. Ledoux, “A language support for cloud elasticity management,” in Proc. IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput., Chicago, IL, USA, pp. 206–215, July. 2014.

[68] M. S. Hasan, Y. Kouki, T. Ledoux, and J. L. Pazat, “Cloud energy broker: Towards SLA-driven green energy planning for IaaS providers,” in Proc. IEEE Int. Conf. High Perform. Comput. Commun., ,pp. 248–255, Aug. 2014..

[69] Y. Gao, Z. Zeng, X. Liu, and P. R. Kumar, “The answer is blowing in the wind: Analysis of powering internet data centers with wind energy,” in Proc. IEEE INFOCOM (Mini Conf.), pp. 520–524, Apr. 2013.

[70] I. Goiri, K. Le, T. Nguyen, J. Guitart, J. Torres, and R. Bianchini, “GreenHadoop: Leveraging green energy in data-processing frameworks,” in Proc. 7th ACM Eur. Conf. Comput. Syst. pp. 57–70, Apr. 2016.

[71] Z. Liu, M. Lin, A. Wierman, S. Low, and L. Andrew, “Geographical load balancing with renewables,” in Proc. ACMGreenMetrics, pp. 62–66, Jun. 2011.

[72] C. Stewart and K. Shen, “Some joules are more precious than others: Managing renewable energy in the data center,” in Proc.Workshop Power Aware Comput. Syst., June 2015.

[73] A. Beloglazov, J. Abawajy, and R. Buyya, “Energy-aware resource allocation heuristics for efficient management of data centers for cloud computing,” Future Gener. Comput. Syst., vol. 28, no. 5, pp. 755–768, May 2016.

[74] A. Verma, “pMapper: Power and migration cost aware application placement in virtualized systems,” in Proc.Workshop Power Aware Comput. Syst., June 2016.

[75] Yichao Jin, Yonggang Wen, And Cedric Westphal, “Optimal transcoding and caching for adaptive streaming in media cloud: An analytical approach”, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 25, No. 12, December 2015.

[76] Zolt_An _Ad_Am Mann, “Multicore-aware virtual machine placement in cloud data centers,” IEEE Transactions On Computers, Vol. 65, No. 11, November 2016.

[77] RuitaoXie, Yonggang Wen, XiaohuaJia, And HaiyongXie," Supporting seamless virtual machine migration Via named data networking in cloud data center", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 12, December 2015.

[78] Ben Martini, Kim-Kwang Raymond Choo, "Cloud manufacturing: security, privacy, and forensic concerns," IEEE Cloud Computing Published By The IEEE Computer Society. Dec 2016.

[79] JasrajMeena, Malay Kumar, Manu Vardhan, "Cost effective genetic algorithm for workflow scheduling in cloud under deadline constraint". September 2016.

[80] Balajipalanisamy, Aameek Singh, Ling Liu, "Cost-effective resource provisioning for mapreduce In a cloud," IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 5, May 2015.

[81] K. Bilal, S. U. R. Malik, and S. U. Khan, "Trends and challenges in cloud datacenters," *IEEE CLOUD COMPUTING SOCIETY*, Sept. 2014.

[82] Ranjithprabhu.K and Sasirega.D, "Eliminating single point of failure and data loss in cloud computing," *International Journal of Science and Research (IJSR)*, vol. Volume 3 Issue 4, p. 2319 : 7064, April 2014.

[83] P. Gill, N. Jain, and N. Nagappan, "Understanding network failures in data centers: measurement, analysis, and implications," *ACM, SIGCOMM, Toronto, Ontario, Canada*, August 15-19, Dec. 2011.

[84] S. K. Khaitan and J. D. McCalley, ``Design techniques and applications of cyberphysical systems: A survey," *IEEE Syst. J.*, vol. 9, no. 2, pp. 350_365, Jun. 2015.

[85] V. Stantchev, R. Colomo-Palacios, and M. Niedermayer, ``Cloud computing based systems for healthcare," *Sci. World J.*, vol. 2014, Art. ID 692619, Apr. 2014.

[86] A. M. K. Cheng, ``Cyber-physical medical and medication systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCS)*, pp. 529_532, Jun. 2008.

[87] I. Lee and O. Sokolsky, ``Medical cyber physical systems," in *Proc. 47th Design Autom. Conf.*, 2010, pp. 743_748. Dec, 2010

[88]R. Sandhu, "Good-enough security: Toward a pragmatic business driven discipline," IEEE Internet Comput., vol. 7, no. 1, pp. 66–68, Jan. 2013.

[89] "Survey and analysis of security parameters in cloud SLAs across the European public sector," European Network and Information Security Agency, 2011-12-19, Dec, 2014.

[90] "Information Technology-cloud computing? Service level agreement (SLA) framework and terminology (Draft)," International Organization for Standardization, ISO/IEC 19086, Dec 2014.

[91] "Cloud service level agreement standardization guidelines, "European Commission, C-SIG SLA, 2015.

[92] J. Luna, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," in Proc. ACM Cloud Comput. Security Workshop, pp. 103–112 Dec. 2012,

[93] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-based quantitative approach for assessing and comparing cloud security," in Proc. IEEE Conf. Trust, Security Privacy Comput. Commun. pp. 284–291, Dec 2014,
.

[94] A. Li, X. Yang, S. Kandula, and M. Zhang, "Cloudcmp: Comparing public cloud providers," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun., pp. 1–14, Dec, 2010.

[95] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for comparing and ranking cloud services," J. Future Generation Comput. Syst., vol. 29, no. 4, pp. 1012–1023, June 2013.

[96] J. Siegel and J. Perdue, "Cloud services measures for global use: The service measurement index," in Proc. Annu. SRII Global. Conf., pp. 411–415, Dec. 2012.

[97] R. Henning, "Security SLAs: Quantifiable security for the enterprise?" in Proc. ACM Workshop New Security Paradigms, pp. 54–60, Dec. 1999,.

[98] C. Irvine and T. Levin, "Quality of security service," in Proc. ACM Workshop New Security Paradigms, , pp. 91–99, Dec. 2011.

[99] S. Lindskog, Modeling and Tuning Security from a Quality of Service Perspective. Gothenburg, Sweden: Chalmers Univ. Technol., Dec. 2012.

[100] V. Casola, A. Mazzeo, N. Mazzocca, and M. Rak, "A SLA evaluation methodology in service oriented architectures," in Proc. Conf. Quality Protection, vol. 23, pp. 119–130, Dec 2006.

[101] S. A. de Chaves, C. B. Westphall, and F. R. Lamin, "SLA perspective in security management for cloud computing," in Proc. IEEE Conf. Netw. Services, pp. 212–217, July, 2010,.

[102] G. Frankova and A. Yautsiukhin, "Service and protection level agreements for business processes," in Proc. IEEE Workshop Service Oriented Comput., pp. 38–43, Dec 2007,

[102] L. Krautsevich, F. Martinelli, and A. Yautsiukhin, "A general method for assessment of security in complex services," in Proc. 4th Conf. Service-Based Internet, pp. 153–164, July 2011.