Journal of Theoretical and Applied Information Technology
31st May 2017. Vol.95. No 10

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

# CRITICAL SECURITY CHALLENGES IN CLOUD COMPUTING ENVIRONMENT: AN APPRAISAL

[1]MOHAMMAD SHUAIB MIR, [2]MOHD. ADAM BIN SUHAIMI, [3]BURHAN UL ISLAM KHAN, [4]M. MUEEN UL ISLAM MATTOO, [5]RASHIDAH F. OLANREWAJU

[1,2]Department of Information Systems, Kulliyyah of ICT, IIUM, Gombak, Malaysia

[3,4,5]Department of ECE, Kulliyyah of Engineering, IIUM, Gombak, Malaysia

E-mail: [3]burhan.iium@gmail.com

**ABSTRACT**

This paper mainly contributes a comprehensive survey on the climacteric security challenges imposed by cloud computing. The paper highlights the challenges/loopholes existing in cloud environment despite all the efforts adopted by organizations, and offers the recommendations for cloud providers as well as users. In this paper, more than 20 research papers pertaining to cloud security, in the span of past 5 years, have been studied and analyzed and twelve most important security threats to organizations have been identified that need attention by research community for encouraging their cloud adoption. This review concludes that some measures have to be adopted for accomplishing complete security in all aspects in the cloud environment. Unlike previous approaches, this effort is directed towards providing a thorough and inclusive review of the security vulnerabilities in cloud. Furthermore, this paper tries to suggest means how cloud federations can enhance security while mitigating risk and building customer trust at the same time.

**Keywords:** *Cloud Computing, Cloud Services, Cloud Service Models, Security Challenges, Threats*

## 1. INTRODUCTION

The concept of cloud computing has shown a rapid progression in recent years owing to the advancements in technology such as virtualization, service oriented architecture and collaboration software. This speedy evolution has resulted in the creation of another corporate periphery which needs to take into account the risks associated with complex relationships on shared platforms. It is the result of this disappearing boundary that business organizations are now working as a portion of a worldwide ecosystem of strategic alliances, supplying franchises and partnerships, rather than in their long-established corporate boundaries. The delivery of remote service and new collaboration standards plus the provision of omnipresent connectivity together with the development in the capabilities of mobile devices have led to the dissolution of customary corporate peripheries and ideas thereby transforming the ways we carry out our work. This shift in paradigms is coercing organizations to look beyond the dependence on Layer 2/3 boundaries and commence with strengthening of conventional weak spaces that revolve around policy enforcement, identity and entitlement. The core infrastructure needs not be abandoned but tiered perimeters should be taken into consideration by federations as well [1].

There has been a tremendous growth in the adoption of hybrid clouds since the last year, as observed by the State of the Cloud Survey, due to the addition of resource pools of private clouds by the public cloud consumers. The survey revealed that the percentage of respondents who adopt private cloud has grown from 63 in 2015 to 77 this year. Moreover, the adoption of hybrid clouds has also reached 71%. Overall, Figure 1 and 2 show that about 95% respondents now use cloud technology as compared to 93% in the previous year [2].

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

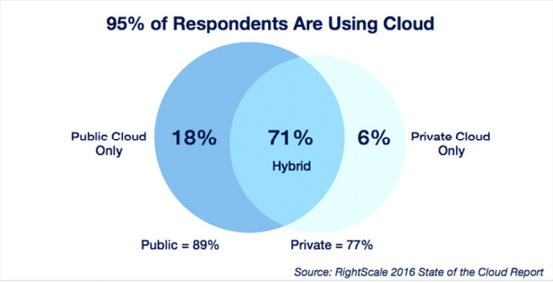


*Figure 1: Cloud Usage in 2016*

*(Adopted from [2])*

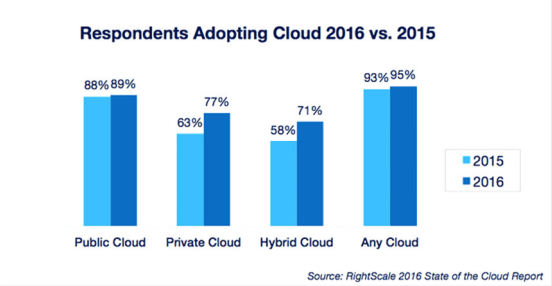


*Figure 2: Adoption of Cloud in 2016 Vs. 2015*

*(Adopted from [2])*

Furthermore, firm-analyst Forrester anticipates that the global market for cloud computing shall show an increasing trend from 2015 to 2020 by moving from $91 billion to a whopping $191 billion. However, this has its own repercussions in the form of security challenges new to federations that used to protect their transactions and critical resources in the garb of restricted partner associations and firewalls [1], [3]. In a cloud computing environment, this can be made to work by employing privacy control and federated identity that shall be discussed in this paper. They will also play an important part in forming the foundation for several security solutions in cloud computing [1].

A comprehensive survey by VMware shows that the decentralization resulting from the shift to cloud computing poses significant security challenges, with 57% respondents worldwide agreeing that it has led to the acquisition of vulnerable solutions by users. Further, about 60 per cent of respondents are in agreement with the fact that decentralization leads to the development of applications external to government or corporate set of laws whereas 56 per cent believe that it leads to absence of regulatory compliance in protecting data [4].

### 1.1 Cloud Computing – The Concept

According to Cearley [5], Cloud computing can be defined as "a style of computing where massively scalable IT-enabled capabilities are delivered as services to external customers using Internet technologies". NIST (National Institute of Standards and Technology, US) states that "cloud computing provides a convenient, on-demand network access to a shared pool of computing resources" [6], [7]. The resources mentioned, here, include platforms, computing infrastructures, network resources, computing applications, virtual servers and software services. Another definition of Cloud Computing was given by Forrester as a pool of abstracted, highly scalable and managed infrastructure capable of hosting end-customer applications and billed by consumption [8][9].

Cloud computing provides the user numerous services such as on-demand access to shared resource pool including applications, networks, storage, servers, as well as services with the least interaction of service provider via internet or management efforts [10]. Notably, cloud computing proves beneficial in providing privacy, scalability, security and economical computing infrastructure that can be availed by the users on demand besides superior quality web based services [11], [12].

Cloud computing assures the user with the following advantages: i) Less cost due to reduction in open corporate investment, ii) Lesser burden of management owing to sharing of responsibilities with Cloud service provider, iii) Extra services on cloud leading to higher responsiveness and efficiency in business, iv) Easily accessible hardware and software resources on cloud, v) Only short-term vendor contracts since users pay on the basis of usage of resources and services [9], [13].

Cloud computing is in its formative years as of now. There is an assortment of cloud service providers, large as well as small, that deliver a range of services. For instance, there are fully developed applications, mail filtering and storage services, support services, etc. In the current state of affairs, most of the IT organizations find the need of cloud inexorable. The applications of cloud like portability, retrieval and storage of data have proved to be highly significant for the ITeS and IT organizations that deal with BigData and cloud computing [1], [14]. Furthermore, IT professionals have gained skill at running various services on cloud under the influence of business requirements. Nevertheless, the world is also witnessing the emergence of cloud computing integrators and aggregators that offer single point of entry into the cloud via product packages and services.

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

Cloud computing gets more interesting to understand when we ponder over the requirements of IT environments today, which include avenues for increasing capacity plus dynamically adding capabilities to cloud infrastructure with no extra cost in purchasing a new one, and no need of conducting training of inexperienced personnel or the requirement of a license for new software. Cloud computing models provide solution to all these needs through services able to be used on Internet encompassing a paradigm based on user subscription or payment as per usage thereby extending the current capabilities of an IT shop. Majority of the users including IT managers find this approach acceptable as they yield profits on their investment [1].

Interestingly, the rate of cloud adoption by organizations has increased in the previous year from a percentage of 43 to 68 in the current year. On the other hand, just 8 per cent companies are willing to shift whole of their infrastructure on cloud in the prospective years. The survey [15] reveals that the topmost security concerns in cloud computing have been found to be denial-of-service (DoS) attacks (34%), malware (37%) and unauthorized access (69%).

Analysis of more than 20 research papers was conducted in this paper that were put forward by researchers in the time span of last five years, which implies that most recent ones have been taken into consideration. This in-depth study in the area of cloud security helped us in outlining the most important security issues in cloud based environment. Some of the works have been highlighted as follows:

The paper [9] summarizes the benefits of using the cloud, provides a brief explanation about the deployment and delivery models and examines in detail the data related issues in the Cloud viz., cost, storage location, security and availability. The point is to bring into limelight some of the foundational knowledge for associations who are ready to relocate to the Cloud to exploit this most recent worldview of computing.

The paper [16] depicts different classifications of issues related to security emerging from the use of services offered by cloud. The authors have talked about security related challenges, for example, security related to data storage, security related to data transmission, security related to application, security for trustworthiness of cloud and third-part resource security. In order to recognize the highly vulnerable nature of cloud security, a threat's probability is also inferred. It can be deduced that in order to boost the progression of cloud computing in the Internet, it is fundamental to reinforce the security capacities.

The paper [17] presents an exhaustive review on the difficulties and challenges related to security in cloud computing. We first investigate the effects of the characteristic attributes of cloud computing, viz., elasticity, multi-tenacity, and control of third parties on security prerequisites. At that point, we investigate the security necessities of the cloud in relation to the central issues, i.e., privacy, availability, integrity, trust, review and consistence. Moreover, the authors here have talked about the nomenclature for security related issues in cloud computing. At last, the cloud computing related security issues have been abridged by cloud security architecture.

The objective of the paper [18] is bipartite; firstly, to assess security of cloud by recognizing exclusive security prerequisites and also try to provide a feasible solution that would obliterate these latent dangers. This paper proposes presenting a Trusted Third Party, entrusted with guaranteeing particular security qualities inside a cloud domain. The solution proposed adjures cryptography, particularly Public Key Infrastructure working together with LDAP and SSO, in order to guarantee the integrity, authentication and privacy of data and communications involved. The provided solution, proposes a service of horizontal level, which will be available to all involved elements, that perceives a security mesh, inside which maintenance of essential trust is observed.

The paper [19] examines the various kinds of technologies for cloud computing and explores their research survey's results that were intended to look into the hindrances that keep the organizations from embracing cloud (with security issues being the center of interest). The respondents of the survey principally favored the utilization of private or hybrid cloud, and this particular stipulation will be actualized in the final product. The work followed in the future will incorporate the advancement and utilization of virtualization in testing of an e-learning instrument, services related to web and platforms that are open sourced to evaluate the possibility of embracing the technology of cloud computing with negligible security risks. The work will advocate the associations that wish to embrace cloud technology. At last, it will assess cloud's efficiency in the learning environment.

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

For the purpose of analysis, the already existing solutions have been taken into account in this paper [20]. The authors have considered different types of attacks that can be found in the cloud. Cloud clients must comprehend and stay cautious about the data breach risks involved in this setting. They recommended another model for enhancing the features of the current model. This work of research focused on rendering a solution for security issues that will enable the cloud users to intelligently prevent the breaches in their cloud storage systems.

Another paper [21], studies the cloud computing data security issues like that of encryption of data, access control, authentication, integrity, etc. It is the view of the authors that the cloud computing security research is in an infant phase of evolution and there are still countless important issues to be considered exhaustively.

In [22], a legislation driven schema is put forward which intends to guarantee access control that perpetuates confidentiality in public clouds while managing personal data hosted by them. Furthermore, the interoperability issue between heterogeneous policies representing the handling of personal data on a cloud setting is discussed in the proposed framework. For this purpose, the access control delegation's need is also shown and taken up. This schema intends to guarantee an access control system that fuses together policies at three levels: the policies of data owner, the policies of the cloud provider and the policies based on legislations. It is believed by the authors that this will help in modelling thorough and undeniable security properties for environments that require interoperability across multiple organizations like that public clouds which are open and dynamic systems with an added level of uncertain and challenging conformity to legislation.

The paper [23] conveys another test to the cloud service provider as it studies about the cloud security challenges and draws a parameter wise correlation of the present security arrangements. In view of these correlations, another security model is put forward which expresses security requirements of the client.

From the viewpoint of clients, security concerns related to cloud computing are yet to be resolved completely, specifically, matters pertinent to ensuring privacy and security of data. In spite of the advertisements by cloud suppliers, claiming that data stays sheltered from security breaches, the loss of data is still a common occurrence due to the attacks on the cloud system [24].

The review [25] identifies the security related issues that emerge because of the open, shared, and virtualized nature of cloud computing archetype. Along these lines, the necessary means are put forward in this paper. A brief discussion of the security related concerns of the MCC has also been included. The resulting discussion brings some open issues into limelight which can persuade the academia and research community to concentrate on the subject.

The paper [26] includes a study on different attacks in virtualization environment with special concentration on possible attack scenarios at every platform. The possibility of attack's nature in cloud infrastructure, i.e. whether the threat is software level or hardware level, has also been identified.

The review [27] basically explores different difficulties faced while dealing with the field of Mobile Cloud Computing (MCC), which includes replication of data, unreliable nature of MCC, consistency, restricted scalability, untrustworthy accessibility to the resources of the cloud, privacy, trust, portability and security. Among the services that use cloud resources ensuring provision of mobile application security and user privacy are of paramount importance as they pose to be the most challenging aspects in MCC. According to the authors, problems related to security of data, location of data, network security, data integrity, authorization, authentication, data access, privacy and confidentiality of data, breaches in data security and other different factors need to be secured in order to ensure secure MCC.

In the paper [28] the center of attention are the issues related to security in relation to cloud computing and methods to tackle the issue of data privacy. In order to tackle the issue of data security, the authors have characterized image steganography and pixel key pattern techniques.

Then, paper [29] identifies various security challenges related to data in cloud based environment and provides solutions to tackle and minimize the risks involved. It is indicated by the authors, that privacy and data security are the most vital and basic factors to be taken into account. It is their belief that in order to ensure cloud computing security concrete standards will be put forward in near future. Advanced encryption schemes that ensure secure access to data can be utilized for the storage and retrieval of data from the cloud.

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

Likewise, for key distribution to cloud users, a proper key management system can be utilized which will allow data access to authorized persons only.

In the paper [30], the issues related to privacy and security in cloud computing have been discussed. This paper, however, concentrates mainly on the issue of data security. Various other features of security along with their solutions as given in literature, for example, availability, privacy and data integrity are also discussed. The aim of this article is to increase the research interest in this field can act as a point of breakthrough for future research.

A brief survey of the technology of cloud computing alongside service and deployment models is demonstrated in the paper [31]. The center of attention of our study is the various security issues related to cloud computing and most of the solutions that are available to tackle these issues have also been listed. Furthermore, the most prominent threats as perceived by cloud security alliance (CSA) have also been listed.

The technical aspects of cloud computing have been thoroughly surveyed in the paper [32]. A general architectural design from specific persons to organizations for cloud computing has also been analyzed in this paper. The fundamental concentration of our study was on security of cloud and deployment of various cloud models. Different threats and security concerns of cloud computing have also been pointed out and duly underscored as with regard to the present scenario security is a rapidly growing concern.

Different security factors have come to forefront in this paper which includes solution of security issues by third party auditors. Second point of focus of our study is the issue of Trust on the service provider of cloud to the level that a company trusts the cloud service provider for administering their organization's data. This review establishes that for the sake of development of cloud technology, trust is an extremely important variable and thus an all-inclusive trust management system needs to be developed. As such, many reputation and trust models were presented and investigated in the paper [33].

Various security challenges, threats, vulnerabilities and attacks that constrain the adoption of cloud computing have been described in the research study [34]. This paper puts forth a crafted review of issues related to cloud security and the various difficulties that emerge from the distinctive features of the cloud such as virtualization and sharing of resources, public nature of cloud and pooling of resources. Furthermore, it's highly likely that governments want development of cloud technologies to enhance the standards of the services in terms of quality, performance, security and innovation. For the purpose of an improved security scheme, a 3-tier architecture model has been put forth. The proposed model discusses the security deliberations at each of the three levels of the cloud service system.

The rest of this paper is organized as follows: Section II discusses the deployment approaches and services offered by Cloud Computing. Sections III and IV provide a detailed discussion on the vulnerabilities in cloud environment and security recommendations for ensuring cloud security. Finally, a brief conclusion has been provided in Section V.

## 2. CLOUD COMPUTING DEPLOYMENT MODELS AND SERVICES

In general, the cloud computing is deployed in the following four possible ways: private, public, hybrid and community Clouds [9].

- Public Clouds are those systems in which the services offered by the cloud are being furnished by third parties while the service providers are responsible for managing and hosting them. At a particular time, numerous enterprises can subscribe on the given framework [11] [12]. This model, being the most exposed one, has a drawback of possessing many inherent security threats which need to be taken into account.
- Community Clouds are like the Public Clouds apart from the fact that this Cloud type has access to a particular group of Cloud users only.
- Private Clouds are in general owned by a certain company for networks operating within the limits of the enterprise and are exclusively used by that organization only. Compared to the Public Cloud, the data is considerably safer in these Clouds. Moreover, the control is increased in these clouds and as such, the potential security concerns have been lessened in comparison to the public clouds.
- Hybrid Clouds are like a blend of Public and Private Clouds (and sometimes community). For a process that is bound to a particular

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

mission, this sort of Cloud framework is more viable due to improved control and company's own management.

Besides providing storage facilities, the Cloud computing model comprises of, normally, services of three sorts: Software Services, Platform Services and Infrastructure Services [35]. Each of these services is identified with the three delivery models, characterized as under:

- Software as a Service (SaaS): This typically relates to preassembled parts of software or complete applications (like an email framework, processing system for payroll, human resource management, processing of databases) furnished as *services*. The clients, in this case, hope for an easy-to-consume functionality [9]. Moreover, the client is relieved of the burden of equipping a device with each application to be utilized by virtue of on-demand use and licensing [1]. Microsoft Office 365, Google Gmail and Google Docs are some of the examples of SaaS vendor services.
- Platform as a Service (PaaS): This service is an extension of the SaaS application model. Sometimes, it is also called "cloudware" and it incorporates work flow facilities for application development, application design, hosting, testing and deployment, besides application services like security, marshalling and web service integration, team collaboration, scalability, persistence, application versioning, database integration, storage, state management, etc. [1]. The clients in this case hope to purchase savings on cost and time [9]. As such, this model is used by clients for creating and deploying their own applications. Google App Engine, Amazon Web Services, Force.com, Microsoft Windows Azure platform and the Elastic Beanstalk are some examples of PaaS vendor services.
- Infrastructure as a service (IaaS): This model relates to infrastructure focused IT resources, like, storage, visualized servers, operating systems, network devices, and so forth and in addition to this, it also includes hardware related services to allow software and Cloud platforms to work. The clients in this case hope to buy computing [9]. A self-sufficient (IT) environment is provided by this model. GoGrid, Rackspace Cloud and Amazon Elastic Compute Cloud (EC2) are some examples of IaaS vendor [36].

## 3. SECURITY VULNERABILITIES AND THREATS IN CLOUD COMPUTING

This segment discusses the difficulties that will be confronted by cloud computing in the future. The greatest difficulties confronted by organizations in adopting the cloud are safe and secure storage of data, standardization, and fast access to the Internet. Many concerns about the protection of data rise when large amounts of data is stored in a centralized location without compromising security, privacy, application specific preferences, and identity of the user [1][13]. These worries, thus, prompt to inquiries regarding the legal framework that ought to be executed for an environment that is cloud oriented [1].

Besides the aforementioned difficulties, the unwavering quality of cloud computing has raised questions about its reliability in technology circles [37]. Issues that happen in the cloud have a tendency to get loads of exposure publicly due to the public availability of the cloud. Not at all like issues that happen in big business situations, which frequently can be contained without reputation, the clients which face problems in cloud computing, howsoever few, stand out to be newsworthy which can be taken care of without coming out to public eye [1].

Remarkably, with the further adoption and standardization of Cloud, the various security issues are escalating too: The privacy and security of data and frameworks remain a top concern in the cloud for 70% of IT experts around the world, which has increased from 63 per cent in 2015. As indicated by Netwrix Corp's second worldwide Cloud Security Survey, loss of control over data is a concern for half of the IT experts (53%) which furthermore found that, despite the fact that cloud specialist organizations prioritize security as a top need, there are still various dangers related to cloud computing, which includes a likely probability for unapproved access by workers and outsiders, invisibility into what is going on across cloud IT environments, and sophisticated attacks. The bulk (61%) of respondents demonstrates that their own workers lay increased threat to data security in the cloud than any other individual. Also, a huge majority (95%) of respondents reflects visibility into activities of the users in the cloud to be an authoritative security component to be provided by the cloud provider [15].

Besides, the GTRA's research likewise demonstrates that the most well-known worry about

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

actualizing cloud projects was privacy and security, an observation which is further bolstered by an IDC investigation in which 75% of respondents recorded security as their main concern. The investigation was carried out on 244 CIOs on cloud computing. Undoubtedly, shifting from designs that were charted out for on-premises services and were under firewalls' security and threat identification frameworks to mobile environments with SaaS applications makes past frameworks unsatisfactory to safeguard data adequately. Moreover, it was found at a March 2009 FTC meeting examining cloud computing privacy and related security issues that like the present day financial meltdown, the data management services may encounter a similar failure, if extra regulation was not executed. To put it plainly, a few managers are essentially frightened, to push ahead with the adoption of implementing the cloud. In any case, this worry, while genuine, is not impossible to surmount. As of now, there are innumerable cases of productive cloud computing executions from all associations, right up to huge venture enterprises that have generally a very low tolerance for the risks, for example, the U.S. Department of the Navy [1]. The security group is additionally meeting up through different initiatives aiming for creating guidance and education. As similar to any developing innovation, the security in cloud environment must go through a learning curve; however it is most likely that case analyses and resources are present in today's world which would help any enterprise to conquer this.

Further discussion reveals more problems in cloud, the alignment and integration of security projects in a cloud domain or a particular enterprise is a major test. The conventional methods of security have centered upon the security of an enterprise and in a way ignored supply chains and ecosystems. Hence, even if a cloud supplier provides a strong security policy and one of its intelligent clients may still possess a problematic data security in totality. Communication gaps, for example, not being able to share the information about a security event flawlessly between the two groups are often found. The interdependencies underlying the adoption of cloud computing are quite captious. Important security deliberations are created in cloud by the simplicity of development utilizing APIs and quick deployment in cloud. SaaS sellers frequently create applications that don't completely cover the security capacities of fundamental IaaS establishments.

Mobile IT clients get access to their business data and services by virtue of cloud based services whilst bypassing the corporate network. Hence, there is immense need for organizations to create controls over security between cloud based services and mobile users. The organizations are prone to large amounts of distributed risks because a lot of important information is stored in the cloud which is globally accessible - the attackers get access to data for stealing from far and without entering the premises of the enterprise which are using cloud services, and in addition to this all the data can be found in one "virtual area". It is required that the virtual machines from various organizations be co-situated on the same physical assets in order to maintain virtual efficiency [1]. Even though conventional security related to data center is equally applicable to the cloud environment, physical isolation and security meant for hardware cannot prevent attacks between virtual machines on a single server as compared to the conventional data center access model where the access is controlled and restricted directly or on premises connection, the access is through the Internet. This makes our system risk prone and calls for a strict observation for any changes in the framework and restrictions on access control. Furthermore, the problem to keep up with security's consistency and guarantee the auditability of records is further aggravated due to the dynamic and fluid nature of virtual machines. The easy way in which cloning can be performed and the distribution between physical servers can result in configuration error propagation and various other vulnerabilities. It will also be equally problematic to prove the security condition of a framework and isolating the area of an insecure virtual machine. The intrusion detection and prevention systems should have the capability to detect malicious activity at a virtual machine level irrespective of the location of the virtual machine inside the virtual environment. Hence, sharing the same location by different virtual machines adds upon the area prone to attack and also increases the threat of virtual machine-to-machine compromise [37].

Conclusively, the security analysis conducted in this paper on cloud computing environment revealed the following twelve issues as the foremost issues that need to be undertaken in near future:

### 3.1 Abuses of Cloud services

As recognized by the Cloud Security Alliance (CSA), abuse and reprehensible utilization of cloud computing is the topmost risk for cloud

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

services. The services provided by the cloud can be hijacked to boost certain nefarious exercises, for example, cracking an encryption key by utilizing resources of cloud computing to start an attack. DDoS attacks, phishing emails and sending spam, and facilitating malignant content are some other examples. A public cloud can be penetrated by an attacker, for instance, and figure out how to transfer malware to other large number of computers and utilize the cloud infrastructure's power to attack other different machines [38].

### 3.2 Data Infringement

The threats found in conventional networks of organizations are equally valid for cloud environments, yet the cloud providers become an alluring target for the attackers because of the vast amount of data stored on the cloud servers. Depending upon the impact of the revealed data, a measure of the seriousness of the potential harm can be made [13]. This can happen due to a variety of reasons, for example defects in designing the application, infrastructure, inadequate authentication, issues related to operation, audit controls, and authorization [39]. It has been revealed by a research conducted by Skyhigh that about 21% of the files that are stored on the cloud servers are of sensitive nature which infers that documents may be considered as intellectual property [40]. Breaches which may include trade secrets, information regarding health, and intellectual property may not make it to the headlines like exposed financial information but these breaches are equally severe and can be more disturbing. It is quite common for consumers to file law suits when their data gets compromised, taking after the legally mandated breach disclosures, hence fines can be implemented on the cloud service provider. At the point when a breach of data happens, fines are incurred on organizations, or may confront criminal charges or lawsuits. The affair of investigation of breaches and consumer notices can pile huge expenses on the cloud service provider. In addition to this, there can be indirect impacts, which can have long lasting effect on organizations, for example, harm to the name of the brand and loss of business.

### 3.3 Multi-tenancy Risks

With the adoption of the approach of multi tenancy in cloud computing, the framework vulnerabilities, or bugs in the programs that can be exploited, pose a bigger problem to cloud computing. Different resources are shared by organizations, such as, sharing memory or databases, in closeness to each other make way to new attack surfaces. As demonstrated at this year's Black Hat security gathering, held in Las Vegas, the research conducted by CloudPassage, it was shown that a huge number of respondents (94%) said that the shift to cloud based framework from the conventional data center environment increases the quantity of workloads on servers, which in turn increases (by a factor of 2 to 100 times) the attackable surface area [41].

### 3.4 Insecure APIs

APIs are basically now being offered by every cloud service and application. APIs are used by IT groups to interact and manage cloud services, which include the services that offer cloud management, provision, monitoring, and coordination. The availability and security of services offered by cloud depend on the security of APIs, right from access control and authentication to encryption and monitoring of activities. With third parties relying on APIs and building on these interfaces, the risks are further increased as further exposure of credentials and services by enterprises may be needed. APIs and poor interfaces divulge associations to security concerns in relation to integrity, privacy, accountability and accessibility [13].

### 3.5 Adoption of Paralyzed authentication

Negligent authentication, poor key or certificate administration and weak passwords frequently result in breaches in data and other attacks. Associations attempt to distribute permissions suitable to the client's job role, and as such often struggle with management of their identities. Moreover, in some cases, they are negligent in removing a client's access when a job function changes or a client quits the association. Verification frameworks that are multifaceted, for example, authentication over telephone, one time passwords and smartcards secure services offered by clouds since they make it more difficult to sign in with stolen passwords which may be attempted by the attackers [36]. The famous Anthem breach, was the consequence of stolen user credentials, and revealed more than 80 million client records. In absence of multifaceted authentication scheme, the attackers could easily breach into Anthem's security. Likewise, numerous engineers commit the error of inserting cryptographic keys and credentials in source code and presenting them in public facing confronting sources, for example, GitHub.

### 3.6 Service, Account and Traffic hijacking

Software exploits, phishing, and fraud are still very effective, and services offered by cloud

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

make these attacks even more effective as the attackers can manipulate transactions, change data and eavesdrop on activities, thus adding new dimensions to the already existing risks. The Cloud application can be utilized by attackers to dispatch different other attacks. Service or account commandeering can be found in the network because of the attacks, such as, fraud, phishing, botnets, software vulnerabilities such as buffer overflow, and Cross Site Scripting (XSS) [39]. CloudFanta, a new malware campaign, has been operating since July 2016, according to Netskope Threat Research Labs and fundamentally targets clients from Brazil. It is observed to be the reason behind stealing of 26,000 email credentials, sending malignant messages masquerading as the victim while screening the e-banking activities. It arrives by means of a link or an attachment in a spear phishing email [42].

### 3.7 The insider malice

If the organizations are unaware of the fact that their employees are utilizing cloud services, those workers can do pretty much anything without anybody knowing — till it's past the point of no return. The insider malice can appear in various forms: a present or previous worker, a contractor, a system administrator, or an accomplice in business. The motivation for malicious activities can range from revenge to data theft. A resolute insider can manipulate data or decimate entire frameworks in a cloud scenario. Different other types of insider malice may include specialist hackers who are executives, wanting unauthorized sensitive data only for the sake of entertainment, and corporate spying that includes theft of top secret data of business for corporate purposes, which is probably seconded by national governments [39]. Notably, frameworks which are at serious risk are those who depend entirely on the cloud service provider for security, for example, encryption [36].

### 3.8 Data loss /leakage

With the subsequent evolution and development of the cloud, permanent loss of data is reported because the supplier's error has become more and more uncommon. Having said that, the hackers who are involved in malicious activities are well known to delete cloud data permanently to damage organizations, and cloud server centers are as helpless against regular catastrophes as any other facility. Data deletion, malicious attackers, loss of data encryption key, corruption of data, natural disasters, or defects in storage systems are the main reasons for the data loss. In the year 2013, about 44 percent of cloud service vendors have confronted brute force attacks that caused data leakage and data loss [39]. The period for which an organization must retain audit reports and other documents is stipulated by compliance policies. Losing information of that sort may have very genuine administrative consequences. Corruption of personal data and destruction of data are also considered as data breaches which need serious notice, according to the new EU data protection rules.

### 3.9 Advanced Persistent Threats

The services offered by cloud can be utilized as a vector of data exfiltration. The Advanced Persistent Attacks (APTs) have been relevantly referred by CSA as "parasitical" types of attack. Over a broadened timeframe, APTs can penetrate frameworks to set up a base, and then sneakily steal information and even the intellectual property. APTs commonly move alongside the normal traffic through the system and mix in with typical activity, so they are hard to identify. Direct attacks, compromised third party networks, spear phishing and USB drives preloaded with malware serve as basic reasons of intrusion. A new research has uncovered that with regard to cloud applications, around seventy five percent of them fall short of the required essential capacities to guarantee consistence with the European Union General Data Protection Regulation (GDPR). Also, the malware in the cloud applications has increased by three times since January. What is more awful is Netskope has found 11% of organizations to have authorized applications bound with malware, implying that since the past quarter the number has nearly tripled [43].

### 3.10Denial of Service

Denial of Service (DOS) is done in order to keep the authentic users from availing the services of the cloud such as accessing storage, network, data and various other services. 81 percent clients consider DOS a huge risk in cloud and DOS attacks have been ascending in cloud computing in last five years [39]. It has been a considerable amount of time for which DOS attacks have been around, yet they have picked up much eminence on account of their presence in cloud computing since DOS attacks usually influence accessibility. Frameworks may suffer to the level of crawling or sometimes fully time out. The report [39] states, "Experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock; there is one way to get to your destination and there is nothing you can do about it except sit and wait". DoS attacks drain a lot of power while processing,

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

which eventually may generate a huge bill which the client needs to pay. Furthermore, Distributed Denial of Service (DDOS) assault is a different type of DOS attack in which various sources of the framework are utilized by the attacker to transmit countless requests to the cloud in order to devour it of its assets.

### 3.11 Shared technology flaws

A critical danger to cloud computing is the vulnerability in shared technology. The companies which provide the cloud services share applications, platforms and infrastructure, and if in any of these layers a weakness emerges, it influences everybody [37]. It has been accounted for, "A single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud". In the event that a fundamental segment of the system is jeopardized for example, an application, a common platform component, or a hypervisor; it can endanger the whole environment to breach and compromise.

### 3.12 Insufficient diligence

The CSA cautioned that the associations that start using the cloud without completely discerning its nature and its related dangers may experience a "myriad of financial, commercial, technical, compliance and legal risks". Considerate thoroughness is needed whether the association is attempting to move to the cloud or blending (or working) with a different organization in the cloud. For instance, associations that neglect to investigate an agreement may not know about the supplier's obligation if there should be an occurrence of breach or information loss.

## 4. RECOMMENDATIONS FOR ENSURING CLOUD SECURITY

In the past section, it is established that the biggest issue in cloud computing is security, especially when we consider the SaaS environment. A senior computer researcher at NIST, Dr. Ron Ross [1], as of late stated, "You're never going to have complete trust. We don't live in a risk-free environment-we have to manage risk, not avoid it." In this section, we will be discussing about process, direction, and practical applications, which can be utilized in any cloud framework to keep the risk at a tolerable level.

Despite the fact that there is a huge advantage to utilizing cloud computing, the various security concerns found in cloud have caused a few associations to delay to migrate their important assets to the cloud. As indicated by Alex Vovk [15], Netwrix CEO and its fellow benefactor, "Lack of visibility is the primary reason why security remains the top cloud-related challenge for many organizations. Advanced security solutions and an integrated view of activities both in the cloud and on premises will help companies increase user accountability, detect insider threats faster and prevent data exfiltration, thus minimizing the damage from unauthorized or incorrect user actions".

On both the individual and organizational level, there is a concern maintaining the integrity of compliance and security in the cloud computing paradigm. What increases the concern significantly, however, is the adoption of cloud computing by the companies while being unaware of the ramifications of putting their important information and applications in the cloud. Migration of their important applications and information is a noteworthy concern for companies who have adopted a shared and public cloud environment and moved past the defense perimeter of their data center. To ease these worries, the provider of the cloud services should guarantee that its clients can keep on having a similar level of security and secrecy regulations over their services and applications, and should give proof to their clients that their association and clients are safe and secure and that their service level agreements are met with, and demonstrate to them how they can establish consistency to their auditors. For the cloud market to advance and flourish, the cloud, in spite of its recent developments, still needs some type of institutionalization and organization [1]. After standardization, communication with each other and interoperation is further facilitated in the cloud environment.

It is critical to understand that enterprises, particularly those from highly regulated industries, own the accountability for their security posture regardless of who actually manages it. Enterprises want a holistic view of this security posture to see cloud as an extension of their on-premise IT footprint. Enterprises and cloud providers need to agree to look beyond organizational boundaries to hold this common perspective. Greater transparency is needed on the part of providers to assist enterprises in managing the myriad of security issues. From governance and compliance to operations, cloud providers have an obligation to lean towards greater disclosure of their activities, while preserving privacy obligations. Cloud provider security is uneven overall, with some providers having excellent security programs and

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

others leaving much to be desired. We must insist upon an industry standard baseline of security for all cloud providers, and we must insist upon a high level of transparency on the part of cloud providers as to their security efforts. Both enterprises and cloud providers need to cooperate with each other to better regulate their security plans, architectures and communications.

Therefore, security assurance is of paramount concern when we discuss the greater good of the cloud computing industry. Among the areas of cooperation and collaboration we feel are important include: i) Threat intelligence and incident sharing ii) Transparency that extends assurances to verifiable controls with strong integrity checks iii) Open interoperable standards development on common security requirements/controls iv) Support for multi-vendor enterprise architectures to assure interoperability, data portability and vendor lock-in avoidance. Cloud providers need to put a greater emphasis on cooperation with their competitors to create greater trust in the industry and to accelerate security solutions.

A focus on greater automation, disposable infrastructure, and agility among other concepts is changing how we deal with problems such as malware, forensics, denial of service attacks and compliance. At the same time, cloud computing does not exist in a vacuum. Complementary innovations such as Mobile Computing, Internet of Things, Software Defined Networks, Big Data and Artificial Intelligence must be understood and integrated into our cloud strategies and frameworks. The often-conservative nature of information security favors clinging to best practices that we understand, but have diminishing value. We need to take a hard look at many of our existing security practices and retire them in favor of new "cloud inspired" approaches that offer higher levels of security. Furthermore, IT industry needs to engage with policy makers, regulatory bodies and their enforcement arms forcefully to help them understand cloud, where risks really lie and solutions that adhere to the spirit of the regulations. It is required to concentrate on creating experts who are more qualified in the field of data security and enhancing the skill sets of the current experts specifically those involved in technologies related to the cloud. In general, this paper presents the following recommendations for cloud service providers as well as users to ensure a secure cloud environment:

- It is essential that organizations who want to unify their selves with a provider of cloud services need to comprehend the safety efforts used by the provider to secure the identity platform. It is considered too risky to concentrate identity into a solitary vault. It is needed by the associations to measure the bargain of the comfort of concentrating identity against the danger of having that storage turn into an awfully valued target for attackers.
- The providers of cloud services for the sake of protecting their environments usually set up security controls, however, in the long run, associations are themselves bound to protect their information in the cloud. It has been suggested by CSA that associations utilize multifaceted confirmation and encryption i.e. multifactor authentication to ensure safety against information breaches.
- APIs and interfaces are normally available from the open Internet and thus have a tendency to be the most vulnerable part of a framework. It is suggested by CSA that one needs to know about the APIs or software interfaces that are being utilized to communicate with the services of the cloud. The organizations are vulnerable to different kinds of security concerns with regard to integrity, confidentiality, accountability, and availability because of the dependence on a weak arrangement of interfaces and APIs. It is suggested by the CSA that satisfactory controls be used as the "first line of detection and defense." It is further prescribed by CSA that figuring out the way by which any provider of cloud one is thinking about incorporates the security all through its service, right from the process of authentication and control techniques for accessibility to action checking strategies. The frameworks and applications modeling threats, which incorporates design/architecture and data flows, get to be distinctly essential parts of the lifecycle of development. Moreover, the CSA prescribes thorough infiltration testing and security-centered code surveys.
- The CSA says that the protection of keys should be suitably ensured, and security of public key infrastructure is of paramount importance. They additionally should be kept on periodic rotation in order to make it difficult for the attackers to utilize keys they have obtained without approval.

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

- It seems we are in fortune, as CSA states that the attacks on vulnerabilities of the framework can be met with "fundamental IT forms". Customary checking of vulnerabilities, promptly managing the patch, and speedy investigation of the observed framework dangers are some of the best practices used for mitigation.
- Organizations ought to keep track of the utilization of the unauthorized services of the cloud and implement Data Loss Prevention (DLP) arrangements in order to control the records and entering of data and departure of the corporate environment. The organizations also ought to make an appropriate approach for security in order to stop portable executable documents with the files of kind "picture/png."
- The expenses of alleviating vulnerabilities of the framework, according to CSA, "are moderately less in contrast to other IT consumptions." In contrast to the potential damage, the cost of setting up IT procedures to find and mend vulnerabilities is quite small. It is suggested by CSA that businesses that are regulated need to fix this problem as fast as possible, ideally as a feature of a computerized and a repeating process. For guaranteeing that the remediation exercises are legitimately archived and looked into by technical groups, change control processes that fix emergency patching are utilized.
- Netskope states that, “The use of cloud services makes the delivery of malware very easy, effectively making it easier to compromise and gain access to users’ data”. It is obvious that it connotes a dire requirement for organizations to utilize a security protocol that is multi-layered with main concentration on services offered by cloud.
- The harm brought about by a security breach can be limited by common defense-in-depth procedures of protection. Associations ought to forbid the sharing of account IDs amongst clients and providers of service, and additionally allow plans of authentication that are multifaceted wherever possible. All accounts, including service accounts, ought to be observed so that each exchange can be followed to a human proprietor. The CSA states that the important factor is to shield the account IDs from theft.
- Also there is a need to apply the best standard practices: On a regular basis, one must store the data and keep versioning on for important constituents of the services of the cloud; clients should be cautioned to abstain from opening attachments that are untrusted no matter what their file name or extension is; a method of two factor authentication should be sanctioned for bank accounts and email as means of security to keep attackers from getting to the email account regardless of the possibility that they know the password; and antivirus and frameworks should be upgraded to their latest versions along with the most recent patches and releases [42].
- It is prescribed by the CSA that associations control the procedure for encryption and keys, minimizing access provided to clients by isolating duties. Also are important exercises like, monitoring, auditing administrator, and effective logging.
- Auditing can be utilized both by the client of cloud services or the supplier of those services. Backup controls, various methods of data library, controls for framework transaction, contingency plans, and framework advancement models are some of the responsibilities of IT auditors [44].
- All of the movement of traffic between the services a client gets in the cloud and the system must go across the Internet. In order to ensure that the information is continually going on a safe channel; one should just associate the browser to the supplier by means of a URL that starts with "https." Also, the information ought to be verified and encrypted utilizing industry standard conventions, for example, IPsec (Internet Protocol Security), that have actually been created particularly to protect the traffic over the Internet.
- By applying stern authentic requirements in contracts while employing any personnel, the danger of having malignant personnel in a CSPs’ staff can be alleviated. An exhaustive examination of the CSP by an outsider, and additionally a dynamic and strong notice system for security breaches will also go far ahead in securing this. As noted by the CSA, it's very common to misinterpret a bungling try to do a job that is quite routine as “malicious” insider activity. As an illustration, one can consider a manager who unintentionally duplicates an important client database to a

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

server that is accessible to public. Legitimate preparing and administration to anticipate such mix-ups turns out to be more important in the cloud because of the more prominent exposure and hence the staff needs to be properly skilled and administration fully prepared to make sure that such mistakes don't happen. To start with, we take into account, precisely, the affectability of the information one is permitting to go in the cloud. Secondly, as per the research company Gartner's recommendation to make it a requirement that suppliers ask for details about the individuals who deal with their information and to what level they can access that information.

- In order to keep APTs from penetrating into their frameworks, the chief providers of cloud services have been using innovative methods for the same, however clients should be as hard-working in recognizing APT imperils in accounts of cloud as they would in frameworks that are on premises.
- In specific, it is prescribed by the CSA to prepare clients to detect the phishing methods. To keep the clients vigilant and alleviate the chances of deception of letting an APT into the system, it is important to regularly run reinforced awareness programs and offices related to IT need to remain educated about the most recent innovative attacks. All these measures, such as, process management, advanced security controls, staff training of IT professionals and occurrence response plans, all prompt to ascend the budget of security. Associations ought to measure these expenses against the possible financial harm perpetrated by effective APT assaults.
- It is suggested by the providers of the cloud services that the information and applications be distributed over numerous zones for additional defense [13]. Satisfactory information measurements for backup are required, and in addition clinging to the best practices in disaster recuperation and business continuity. It is imperative for cloud environments that backup of information be taken on a day by day basis and to make it more secure, the storage should be off-site. The provider of cloud services is concerned with the liability of securing loss of information. In the event that a client encodes information before transferring it to the cloud, then that client must be extremely careful so as to make sure that the encryption key is safe, because the loss of key means the loss of information.
- If an organization's development group is not completely aware about the advancements in cloud technologies, architectural and operational issues emerge as applications are sent to a specific cloud. The associations are being reminded by the CSA that they should exhibit considerable hard work in order to comprehend the dangers they accept while subscribing to every service of the cloud.
- Providers of the cloud services are needed to distinguish different sorts of attacks, for example, investigating traffic to identify DDoS attacks, and put forward instruments for clients to observe the strength of their cloud environments. The survey also revealed that many businesses are not taking advantage of automation tools. Just 28% of respondents said they use a full suite of tools that enable them to secure and audit cloud server workloads automatically when configuring and deploying them. Just over one-third of respondents said they use "some" security automation tools for configuration and deployment, while 35% use nothing [41]. Clients ought to ensure themselves that the supplier of their services offer a method for describing misuse. Despite the fact that the clients may not be the immediate victims of malicious activities, mishandling of cloud services can yet outcome as issues related to service availability and loss of information.
- While it is quite normal to observe large amounts of DDoS assaults, associations ought to know about asymmetric, application level DoS assaults, whose goal is to aim for the vulnerabilities of database and web server. The CSA states that the providers of cloud services have a tendency to be better ready to handle DoS assaults than their clients. The important thing is to have an arrangement to moderate the assault before it happens, so resources are available to the managers when required.
- It has been suggested by the CSA to employ a defense-in-depth technique, which includes multifaceted verification for all hosts, framework based and host based interruption identification systems, to apply the idea of slightest benefit, division of network, and fixing shared assets.

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

## 5. CONCLUSION

Cloud computing on its own is in a growing phase and subsequently the security recommendations are also evolving. It is apparent that even the main service providers of the cloud, for example, Google, Amazon, and so on are confronting numerous difficulties in security and are not steady yet. Accomplishing complete answer for lawful clients is still ambiguous. With such amount of concerns confronted in cloud computing, choices whether to adopt cloud computing or not by a particular association has to be reached in view of the advantages to risk proportion.

## ACKNOWLEDGMENTS

This work was partially supported by Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) under Research Initiative Grant Scheme (RIGS) number RIGS 16-357-0521.

## REFRENCES:

[1] Rittinghouse JW, Ransome JF. Cloud computing: implementation, management, and security. CRC press; 2016 Apr 19.

[2] Weins K. Cloud Computing Trends: 2016 State of the Cloud Survey. Cloud Industry Insights. 2016 Feb.

[3] Jisha G, Samuel P(auth.), Abraham A, Mauri JL, Buford JF, Suzuki J, Thampi SM(eds.). Cloud computing security issues and challenges: a survey. Advances in Computing and Communications: First International Conference, ACC 2011, Kochi, India, Proceedings, Part IV, Communications in Computer and Information Science 193, Springer-Verlag Berlin Heidelberg; 2011 Jul 22-24, 445-454.

[4] Seals T. UK IT Pros: 'we're losing control over cloud services'. Infosecurity Magazine. 2016 Nov.

[5] Cearley DW. Cloud computing: key initiative overview. Gartner Report. 2010.

[6] Mell P, Grance T. The NIST definition of cloud computing. Communications of the ACM. 2010 Dec 10;53(6):50.

[7] Amrhein D, Quint S. Cloud computing for the enterprise: part 1: capturing the cloud. DeveloperWorks, IBM. 2009 Apr;8.

[8] Rhoton J. Cloud Computing Explained: Implementation Handbook for Enterprises. Recursive Press. 2010.

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

[10] Gnanavelu D, Gunasekaran G. A Survey on Cloud Computing Data Storage Security Issues. International Journal of Computer Technology and Applications. ISSN: 2229-6093. 2014; 5(2): 389-392.

[11] Angadi AB, Angadi AB, Gull KC. Security Issues with Possible Solutions in Cloud Computing-A Survey. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). 2013 Feb 28;2(2):pp-652.

[12] Umaeswari P, Shanthini B. Achieving Secure Data Access in Cloud Computing. Middle-East Journal of Scientific Research, 23 (Sensing, Signal Processing and Security): 363-369.

[13] Khan BU, Baba AM, Olanrewaju RF, Lone SA, Zulkurnain NF. SSM: Secure-Split-Merge data distribution in cloud infrastructure. InOpen Systems (ICOS), 2015 IEEE Conference on 2015 Aug 24 (pp. 40-45). IEEE.

[14] Khan BU, Olanrewaju RF, Altaf H, Shah A. Critical insight for mapreduce optimization in hadoop. International Journal of Computer Science and Control Engineering. 2014 Apr 22;2(1):1.

[15] Seals T. Cloud security a top concern for 70% of IT Pros. Infosecurity Magazine, 2016 Nov 16.

[16] Meetei MZ, Goel A. Security issues in cloud computing. InBiomedical Engineering and Informatics (BMEI), 2012 5th International Conference on 2012 Oct 16 (pp. 1321-1325). IEEE.

[17] Tianfield H. Security issues in cloud computing. In2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2012 Oct 14 (pp. 1082-1089). IEEE.

[18] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation computer systems. 2012 Mar 31;28(3):583-92.

[19] Moyo T, Bhogal J. Investigating Security Issues in Cloud Computing. InComplex, Intelligent and Software Intensive Systems (CISIS), 2014 Eighth International Conference on 2014 Jul 2 (pp. 141-146). IEEE.

[20] Beulah S, Dhanaseelan FR. Survey on Security Issues and Existing Solutions in Cloud Storage. Indian Journal of Science and Technology. 2016 Apr 14;9(13).

[21] Yu C, Yang L, Liu Y, Luo X. Research on data security issues of cloud computing. InIET

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

Conference Proceedings 2014 Nov 8. The Institution of Engineering & Technology.

[22] Belaazi M, Rahmouni HB, Bouhoula A. Towards a legislation driven framework for access control and privacy protection in public cloud. InSecurity and Cryptography (SECRYPT), 2014 11th International Conference on 2014 Aug 28 (pp. 1-6). IEEE.

[23] Thakare VR, Singh KJ. A Study of Security and Privacy Issues at Service Models of Cloud Computing. Indian Journal of Science and Technology. 2016 October;9(38).

[24] Shariati SM, Ahmadzadegan MH. Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection. In2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI) 2015 Nov 5 (pp. 1078-1082). IEEE.

[25] Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences. 2015 Jun 1;305:357-83.

[26] Balaji K, Kiran PS. A Review on Cloud Security Challenges and Issues. Indian Journal of Science and Technology. 2016 Nov 22;9(43).

[27] Kulkarni P, Khanai R. Addressing mobile Cloud Computing security issues: a survey. InCommunications and Signal Processing (ICCSP), 2015 International Conference on 2015 Apr 2 (pp. 1463-1467). IEEE.

[28] Kaur R, Kaur J. Cloud computing security issues and its solution: A review. InComputing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on 2015 Mar 11 (pp. 1198-1200). IEEE.

[29] Rao RV, Selvamani K. Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science. 2015 Dec 31;48:204-9.

[30] Arjun U, Vinay S. A short review on data security and privacy issues in cloud computing. InCurrent Trends in Advanced Computing (ICCTAC), IEEE International Conference on 2016 Mar 10 (pp. 1-5). IEEE.

[31] Bokhari MU, Shallal QM, Tamandani YK. Security and privacy issues in cloud computing. InComputing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on 2016 Mar 16 (pp. 896-900). IEEE.

[32] Gandhi K, Gandhi P. Cloud computing security issues: An analysis. InComputing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on 2016 Mar 16 (pp. 3858-3861). IEEE.

[33] Harbajanka S, Saxena P. Survey Paper on Trust Management and Security Issues in Cloud Computing. In Symposium on Colossal Data Analysis and Networking (CDAN), 2016. IEEE.

[34] Singh S, Jeong YS, Park JH. A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications. 2016 Nov 30;75:200-22.

[35] Olanrewaju RF, Khan BUI, Mir RN, Baba AM, Anwar F. DFAM: A Distributed Feedback analysis mechanism for knowledge based educational big data", Jurnal Teknologi. 2016; 78(12-3): 31-38.

[36] Olanrewaju RF, Khan BU, Baba A, Mir RN, Lone SA. RFDA: Reliable framework for data administration based on split-merge policy. In SAI Computing Conference (SAI), 2016 Jul 13 (pp. 545-552). IEEE.

[37] Fernandes DA, Soares LF, Gomes JV, Freire MM, Inácio PR. Security issues in cloud environments: a survey. International Journal of Information Security. 2014 Apr 1;13(2):113-70.

[38] Srinivasamurthy S, Liu DQ. Survey on Cloud Computing Security–Technical Report. Department of Computer Science, Indiana University Purdue University Fort Wayne. 2010 Jul.

[39] Kazim M, Zhu SY. A survey on top security threats in cloud computing. Int J Adv Comput Sci Appl (IJACSA). 2015 Jun;6(3):109-13.

[40] DLP (Data Loss Prevention) in the Cloud. https://www.tclouds-project.eu/2016/05/]. Date accessed: 10/01/2016.

[41] Evans S. Cloud Use Increases Attack Surface, But Security Not Keeping Up. Infosecurity Magazine, 2016 Aug.

[42] Seals T. CloudFanta Malware Uses Popular Online Storage App to Infect Users. Infosecurity Magazine, 2016 Oct.

[43] Seals T. Cloud App Woes: No GDPR Compliance, Malware Triples. Infosecurity Magazine, 2016 Jun 10

[44] Patil Madhubala R. Survey on security concerns in Cloud computing. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). 2015,(pp. 1458-1462). IEEE.