A REVIEW OF THE SECURITY ISSUES IN CLOUD COMPUTING AND ITS REMEDIAL ACTION

Muhammad Waqar Khan[1*], Sumaira Yousuf Khan[2], Sahar Altaf[3], Muhammad Wajahat Ali[4]

[1]Senior Lecturer, College of Computer Sciences and Information Systems, Institute of Business Management, (IoBM), Pakistan.*

[1]Ph.D. Scholar, Faculty of Engineering Science and Technology, Hamdard University, Pakistan

[2]Assistant Professor, College of Computer Sciences and Information Systems, Institute of Business Management, (IoBM), Pakistan.

[3]Assistant Professor, College of Humanities and Sciences, Karachi Institute of Economics and Technology, PAF KIET, Pakistan.

[4]Senior Lecturer, College of Computer Sciences and Information Systems, Institute of Business Management, (IoBM), Pakistan

Abstract: In the recent years, cloud computing has become a widely utilized revolution in the field of data modernization due to its favorable circumstances like high processing power, less expense of administrations, elite adaptability, unwavering quality and accessibility. It is an integral tool that improves the cost of equipment, controllability and utility to share the information and so forth numerous organizations are turning their applications and administrations on the cloud. It offers secure and versatile administrations but in every case there exists some cloud security and protection issues when information has sent from a focal stockpiling worker to an alternate cloud, individual and private information augment the danger of information secrecy, respectability, accessibility, and verification before one pick a merchant in the cloud or pick the cloud and move services in the cloud. In this research, paper several articles are reviewed that deals with the security issues and the remedial actions and responses that have been taken by researchers and organizations in the field of cloud computing. This analysis provides insight to future research opportunities to students, researchers, publishers and experts and help them to study current research trend and security issues related to cloud computing.

Keyword: Cloud Computing, Cloud Computing Security, Cloud Computing Attacks, Cloud Computing Issues, Cloud Computing Needs, Cloud Computing Responses

Introduction

The term cloud in cloud computing is the group of networks like in conventional clouds, the cloud is the pool of water molecules [26]. According to National Institute of Standards and Technology (NIST),” cloud computing is a model that enables convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can easily be managed and utilized with minimum management efforts or cloud service provider interaction” [3]. It is the state-of-the-art information system procedure that offers dynamically shared resources over the Internet and provide economic benefits.

The “cloud computing” evolves from the spur of already established virtual private networks(VPN) that were adapted by providers for providing their services in data communication networks [1]. It has a resemblance with respect to virtualization scenario that exists in cloud computing sharing resources via internet as a virtual environment. Cloud computing offers the facilities which include software, data computation, and storage services and data access. This technology is not concerned with the end-user knowledge of the physical location but well known to the configuration of the system that is providing the facility. It is a newly evolved term in the computing world that vanished the concept of having large data centres at physical locations. It moves the physical equipment of storage, computation, and server facility to the third party large data centres [2]. Cloud computing revolutionized the concept of distributed computing paradigm which is used for profoundly versatile asset pool, stockpiling and registering assets [4]. And for some users, it is a service to access software and store data, for others it is a package that offers the modified form of distributed model in ‘’cloud computing’’ [5]. It attracts all the fundamental elements of society which includes industry, academia, and businesses to reduce their overall cost of regular maintenance.

In the world of IT this novel form of computing is hitting all the fronts with its benefits and adaptability of modifying existed on going procedures without being hesitant. Due to its importance, it also creates more risks and attacks towards the cloud model. It attracts the attackers and hackers to work for finding

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

flaws and loop holes in the existing security architecture of cloud computing services model. Recently many researches reviewed security issues in cloud computing [23],[24],[25]. Instead, of benefits and advantages there are lot of open issues and vulnerabilities which have to be addressed in near future to make this technology more trustworthy and credible with respect to its security parameters. There are multiple issues related to the security of cloud computing model such as [7]:

- Safety measures in cloud
- Credibility of Vendor
- Risk of Multi-Tenancy in Cloud
- Safe and sound Data supervision
- Examine level of portability
- SLA managing system

These are some of the open research problems for the cloud computing model. The main concerned for the adoption of cloud computing security factor plays a key role to the user's perspective [8], because of following reasons:

- Loss of control [9] – transfers the security management to third party source without the knowledge of stored data location and adopted security parameters to access the data.
- Multi-tenancy[3][6][10]– different tenants working in same umbrella with respect to logical and/or physical medium
- SLA [11] - level of expectation at service level agreement should meet with the availability of access of stored data at any time.

The purpose of writing this paper is analyzing the whole cloud computing model security issues. The specific objective is to describe and identify the various attack vectors and security issues related to cloud models. Thus, we analyze all the weakness and flaws and highlight their root causes. This research will help cloud users, developers, providers etc. the concept and understanding in implementation and uses of the cloud security issues. For this sake, we introduce counter attack measures to remain proactive and risk free in using cloud computing. For elaborating the issues first, we give the introduction about the architecture related to security issues and also the key cloud security implications and research challenges which are important to security issues in cloud computing model.

Literature Review

A. Cloud computing Security Issues

There are three services given by cloud computing that are Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS).The fundamental instances of distributed computing which are utilized by wide range of individuals in daily life are YouTube, Facebook, Gmail and Dropbox and so forth .It offers versatility, adaptability, readiness, and straightforwardness due to which its utilization is promptly expanding in the enterprises.

A set of networks, organizations, stockpiling, administrations, and interfaces which empower the on time conveyance of requested services is a Cloud. Over the Internet provision of programming and storage, cloud computing is broken down into three distinct classes:

a) **Private cloud:** a cloud platform that delicately designed for specific organization [41].
b) **Public cloud:** common availability for accessing users to register and use the available infrastructure [40].
c) **Hybrid cloud:** a dedicated private cloud that create access to the resources of public clouds [43], [46].

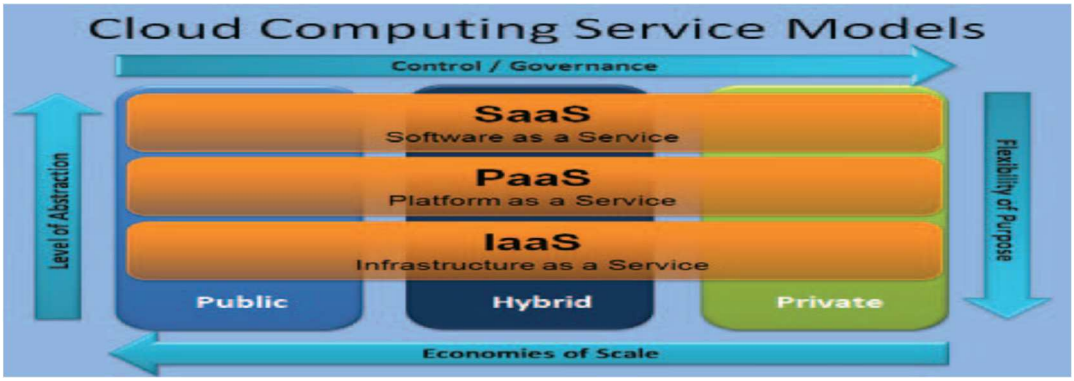


Figure 2. Cloud deployment model-services and delivery [7]

The newly arrived Web 2.0 and cloud technology has boosted up the phenomena of population connected services. Thus, according to Cisco, the IT world is just going towards the objective of availability of everything on internet (IoE) [21]. The transition of IT industry towards cloud environment plays a vital role in achieving the objectives, therefore the initial research papers introduced the concept of service delivery models in cloud computing[4], [6],[12],[13],[14],[15],[16],[17],[18],[19],[20].The

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

models used for delivering cloud services are as follows:

A. Infrastructure–as-a-service (IaaS): In this service the cloud provider delivers the service of computation, service of storage and network resources [38],[39]..

B. Platform-as-a-service (PaaS): In this type of service the cloud provider delivers the environment of platform, as well as tools and authorized users to develop their business services and deploy them according to their scenario which provides easiness to manage their applications [45].

C. Software-as-a-service (SaaS): This is a full package that offers services from ground level by using physical infrastructure services [19]. Thus, can be provided by cloud providers for application implementation.

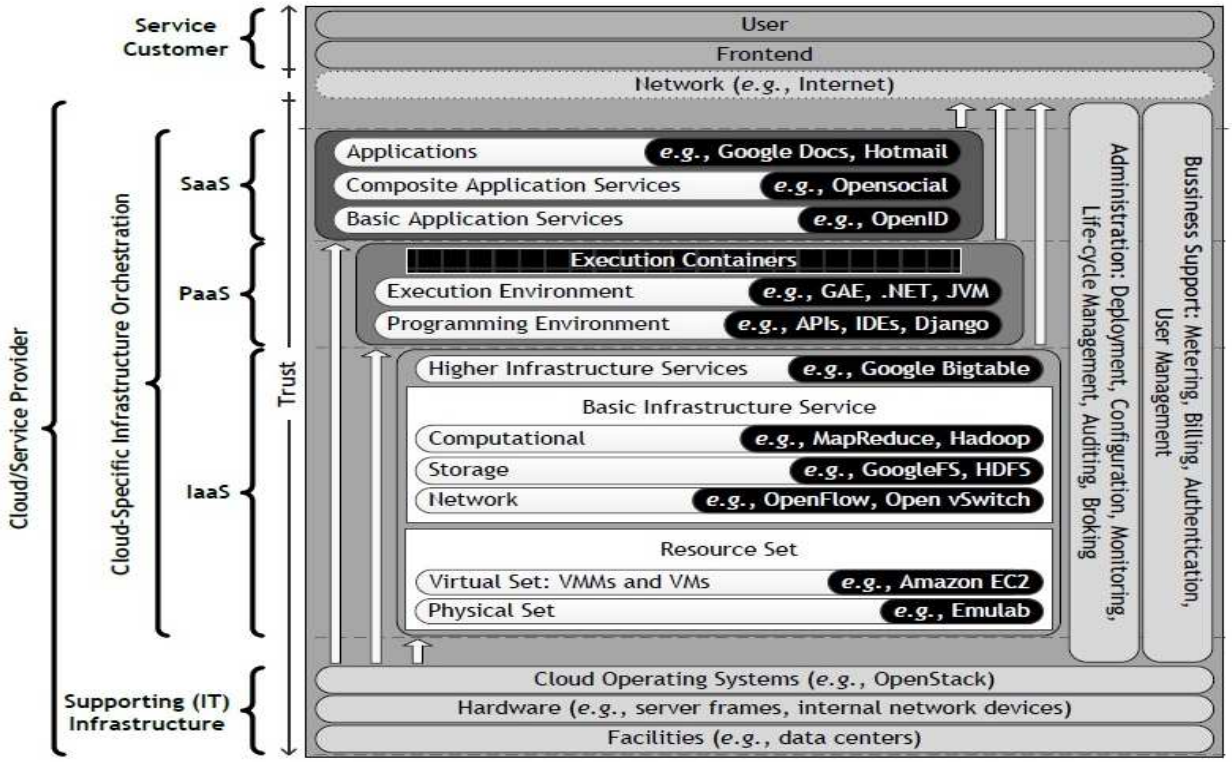


Figure 3. Cloud service delivery models (bottom layer to top user interface layer) [20],[28],[29],[30],[31]

According, to the above services and models in cloud computing, the implemented models and services are

totally dependent on the scenarios respectively. But, the common parameters that are standard in each of these models and services have to adopt by the cloud providers for delivering facilities of cloud computing to the users [5],[8]. Since it provides more extensive, composite and indefinable process without a standard platform to implement the security in cloud. The core objective is to address these security issues and requires feasible improvement in resolving these threats that exists in cloud structure which are discussed in this research paper.

We focused on the following basic components that are fundamental to security issues in cloud computing.

- Risk of Multi-Tenancy in Cloud
- Elasticity in cloud services
- Availability of Information (SLA)
- Secure Information management
- Information Integrity and privacy
- Cloud secure federation

The relevant survey conducted by enterprise panel of IDC, shows the concerns and risks in the mind of users that are very common. The graph below shows the parameters along with the percentage of issues that has been faced by different companies and organizations in adopting cloud computing technology.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

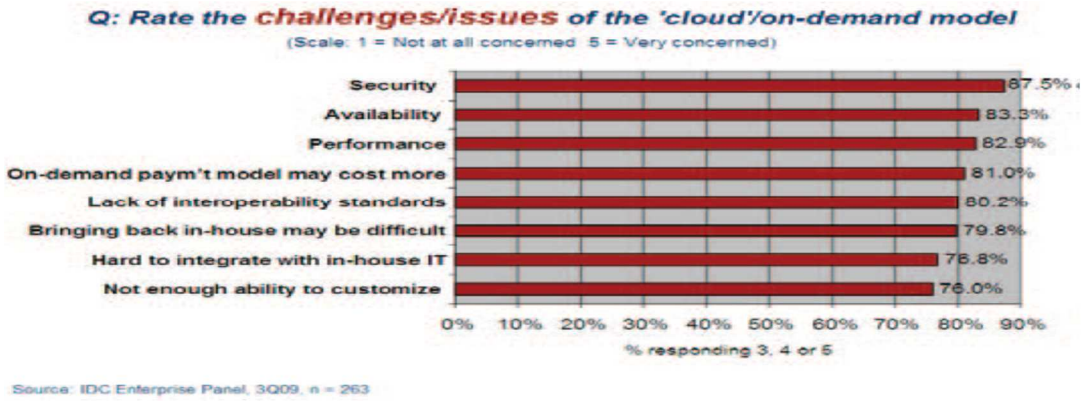


Figure 4. Cloud Computing Security Issues [22],[15]

This remarkable technology has many benefits such as flexibility and elasticity [8], which is the backbone for adapting cloud. Therefore, the security of data transactions, information and processes is at risk when the above-mentioned security issues arises. It is like a hand shake between the cloud user and cloud provider for maintaining trust between them and ensuring the security in all interconnecting scenarios [23].

The next section will elaborate the implications and remediation of cloud security issues.

B. ***Cloud security implications and remediation***

In view of user, this new technology is very dynamic with respect to its deliverables and fulfilling needs on demand. In order to provide this facility to users more complexities are included that can be managed with the help of cloud providers. It includes multidimensional processing of data, multi- tenant approach, availability of on demand computing, available expandable memory and many other facilities. Hence, for user facilities, it is difficult to establish security every time at all places with the same appropriate level [24].

i. Risk of Multi-Tenanc in Cloud:

The various facilities that are available now days in cloud environment include storage availability, attraction of shared computing, availability of shared memory and the window for accessing the unlimited resources that was not possible till the evolution of cloud. To achieve such targets, the cloud provider has to bear the cost of providing these facilities to their users as per their requirements. On the contrary, it is the phenomena of multi-tenant approach for accomplishing win-win condition. Due to this, the providers have to make resources available according to the requirements of the user in a cost effective way, which is not possible without adopting the multi-tenant approach in cloud technology. Thus, every cloud provider has to adopt the cost manageable techniques for running its business or organization.

The below figure shows the multi-tenant approach in which different users or tenants from different physical locations are connected with same physical equipment or logical access, hard drives, data base, equipment for computing and other services. This approach is an open violation of tenant's confidentially personal firm IT assets which alarms the IT world and cloud providers to ensure the security used in multi-tenant approach [10]. For securing cloud, there must be a segregation between the data boundaries of the tenants, because without creating this barrier it is impossible to keep an eye on the flow of data between the data transactions of different users with same physical equipment.

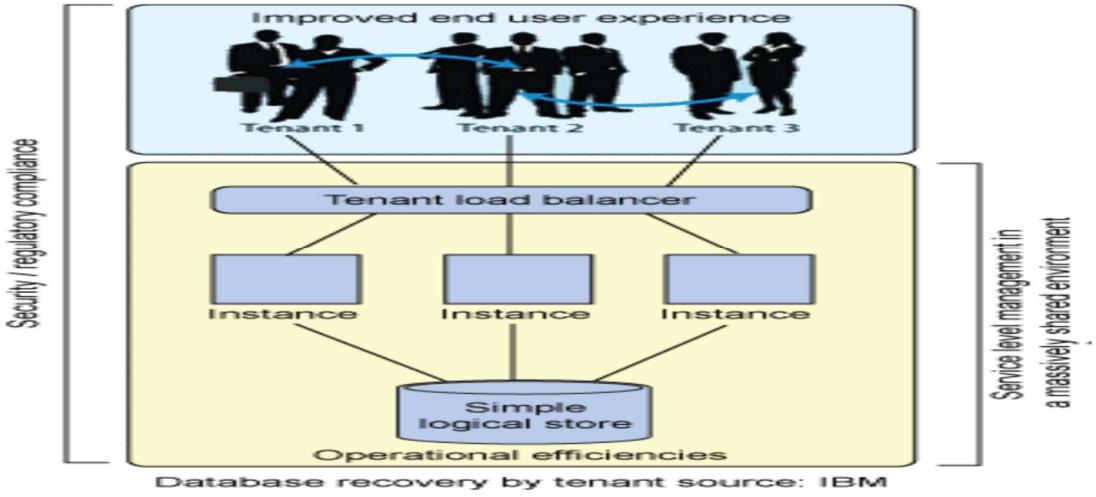


Figure 5. Model of Cloud Multi-tenant approach [7]

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

To provide secure services at user's end there should be an isolation barrier between all the tenants that are using the same-shared physical equipment. In addition, the providers must treat all the tenants equally by not giving any knowledge about their destination of physical equipment that are being used or shared with other tenants. This effort of isolation enhanced the security level against the external and internal attackers from tempering the data of tenants [25]. As this isolation scenario is implemented in infrastructure-as-a-service (IaaS) environment which isolates user's specific virtual storage, as well as their memory, running computing partition and allocate dedicated network paths for access. And so, in platform-as-a-service (PaaS) environment this tactic is also implementable in security perspective for the ongoing services and as well as the scenario of multiple virtual operating systems running on same base operating system. As this virtual platform (VP) is capable of using different programming languages which include NET, Java Virtual Machine (JVM) and many other languages [26]. If, we neglect the precaution of isolation than the multi-tenancy feature initiated a risk factor in the form of modification, replacement and deleted out the tenant's data at the shared physical hardware. The isolation factor is considered more important and implacable in Service-as-a-service (SaaS) environment. In addition, there is a huge transaction of data and information performed by different tenants at the same interval of time. The tenant also ensure the security of the data provided to cloud according to their organizations internal policy for placing their data in isolation with the other tenants of the provider. Also, organization has to modify its policy in need of time and always be in contact with the cloud provider to remain satisfied with their security policies and controls [27].

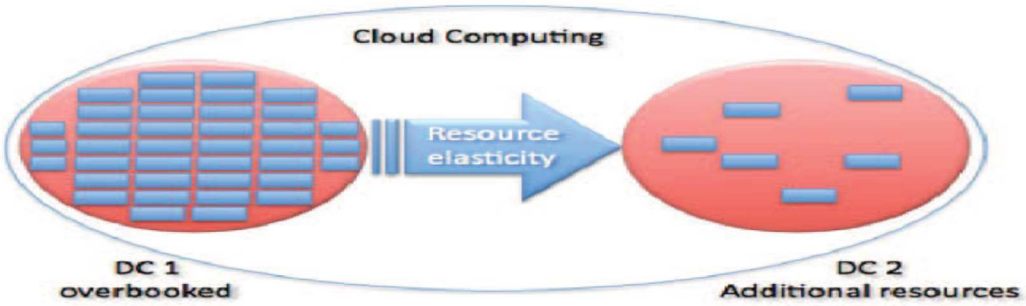


Figure 6. Cloud Resource Elasticity [7]

ii. Elasticity In Cloud Services

Another important parameter in cloud computing environment is elasticity [10]. The word elasticity used in cloud perspective is termed as the availability of scaling up or down for the existing services used

by tenant. The option of modifying the scale according to the demand and time is very useful for user in cost deduction. However, this elasticity arise risk factors for organization to scale down the services. So, it has to release the resources which they are currently using. Even after formatting the assigned resources some of the loop holes still exist that makes the hope of the attackers to leak out the data from the left down resources by the previous tenant. This is one of the major threats to organizations for dealing with cloud environments.

However, nowadays it is not an easy task to recover data from the released resources by the previous tenant. The use of modern mechanism and technique make this phenomenon near to impossible. It uses a service placement engine that update and record the list of existing available resources from the total resources the provider has. The method uses the list to assign resources to every tenant specifically related to its last activity of scaling up or down for ensuring the security perspective. This engine also has a system to avoid the same field competitor request for hiring the same physical equipment used by its competitor, which enhance its level of security. In an ideal condition the physical hardware should be located within the tenant's country line. Since there is another function of migration that exists in the system functioning of cloud environment which accelerates when the engine makes a migration strategy where the local services migrated from the physical equipment to logical host to different destination. Sometimes, migration takes place for the re-enforcement of prescribed security policy by tenants to fulfill the demands and use of available resources in an efficient way.

iii. Availability of Information (SLA):

It is a new technology of cloud computing that has gained popularity day by day in the IT world. But, on the other hand the organizations that are adopting the cloud technology must estimate the security risk and non-availability percentage for their data stored in the cloud [23]. They have to guarantee the backup of the cloud data at their personal internal storage when

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

needed mostly in the case of non-availability. This possibly happened as a result of attack or any break down or any mishap occurred at the physical location of cloud provider where data is stored. Now a days, world information or data is the most important thing because most of the times businesses of organizations are relying on them due to which it needs more security than any other thing.

Figure 7. Cloud Service Level Agreement [33]

Improvement can be done by two joint ways for the purpose of non-availability of information. For establishing, a trust factor between cloud provider and user, (SLA) plays a key role [16], [11]. It defines the risk factor of user in services perspective and decreases the risk factor as the percentage increases which usually exist between the ranges of 98% to 99% [11]. Figure 7 shows the low risk factor for non-availability of resources or services but it existence creates a doubt in organization's mind. To ensure the availability of resources or services by having a backup is another solution for improving the issue of non-availability. The cloud service providers [17], [18], [19] are totally responsible for any down time and to facilitate the users by providing them a system for monitoring and notifications for possible remedial actions.

iv. Secure Information Management:

This is the essential part for improving the security in the cloud world and the layer which works in cloud architecture named as CML (Cloud Management Layer) is the microkernel which unmitigated to include and manage various units. It includes the monitoring of provided cloud service, and parameters of billing, administration of security in cloud and adding name services. As it is vital layer for security purpose. if, any loop hole exists in this layer then the security of other layers would not be able to cover up the intensity of attacks and to stop the breach of unwanted users. Consequently, the attacker will control the whole system by changing administrator rights of the whole cloud platform. This layer is responsible for the back support of user interface layer by offering many APIs for user comfort for the integration with cloud provider platform. In various scenarios the task of monitoring and visual lance on the users' transactions is difficult for the cloud providers due to increase in number of transaction of tenants. To fulfill the purpose of security management with the available resources has become a more critical research problem. For establishing trust worthy relationship with cloud users, the cloud providers should provide the security management plan by keeping in mind the security requirements and security policy of the specific organization. To reduce the security concerns for the respective organization by particularly emphasizing on the key security issues that they are concern a lot for them. And by taking regularly feedback for the security factor of the services they are using in cloud environment. However, the providers have to ensure the cloud users for providing the risk free cloud environment.

v. Information Integrity and Privacy:

The revolutionary computing comes up with the great admiring benefits for IT world. It offers the resources openly for the tenants as the medium on internet where user can access the services provided by the cloud provider. As not only valid users can access these services but also un valid malicious activist and attackers could breach [23],[34]. These services can be used by tenants through their web browsers, as well as it includes many protocols. However, an organization started to link with cloud environment. The cloud provider has to provide the trust worthy secure transactions for its business incentive [34]. When at security perspective the issue related to integrity and privacy exploit due to the loophole that exists in the design and architecture of providers cloud environment [32]. Like, CML, SOAP, VPN, APIs [32] and many others. The major issues related to privacy and integrity are following:

- Unavailability of authority, controls related to accounts not present and omnipresence of authentication
- Un-availability of proper mechanisms for encryption and decryption.

This issue is still debatable between tenants and cloud provides is the trust deficiency that not even fully established of the organizations in the IT world. To overcome this deficit both the ends have to adopt some efforts to establish the relation of trust between

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

each other. As at the user end the use of efficient methods of encryption and other different way of hiding the data that they are storing in cloud. If these efforts would take from the user end then this will facilitate a lot to fulfill the concern of full proof security. And also at other end of cloud provider, they make sure the tenants by increasing the security levels, by adopting multi check for users at the time to access their account and data stored at cloud provider's location. The access of information from user end allows one user at one accessing instant that have to assure by the provider. The providers should adopt the latest encryption mechanisms [35] like RSA certificates mechanism and provide the concept of key and shuffle of it to secure access of user to its respective account by giving update the users of latest monitoring data transactions of their account.

vi. Cloud Secure Federation:

The fast change in technology facilitates the world in a revolutionary manner. And the end user, who do not have knowledge about the services and its issues of cloud computing only have the desire of comfort service with full proof security offered by the provider. So as the responsibility doubled on cloud provider to provide best services with security. The user which uses cloud environment that provided by cloud provider in the form of platform applications and other services that the security of users data transaction is entirely depend on the security of cloud and the levels of path that are located between that connection. It is not being very complicated at normal scale organization but at large scale when number of clouds integrated with each other that provided a big pool of resources or services to users. To make possible to provide security it requires to be federated and enforce with respect to physical and logical and to maintain their security in different cloud platforms like PaaS, IaaS, SaaS. The issue of identity plays an important role in any communication or access to any particular account for accessing information that also happen in cloud transactions for any platform or services of cloud. And these platforms designed on multifarious orders of functioning and reliable access ability that create issues related to transport and for addressing the security issues by using different identify tokens and protocols using for identification [36]. To fulfill all the parameters of security, it includes some major parameters like user identity [7]. That plays an important role in security environment

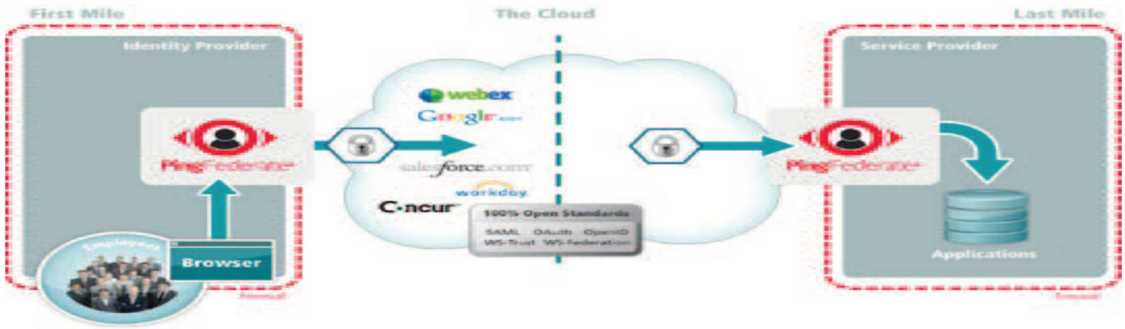
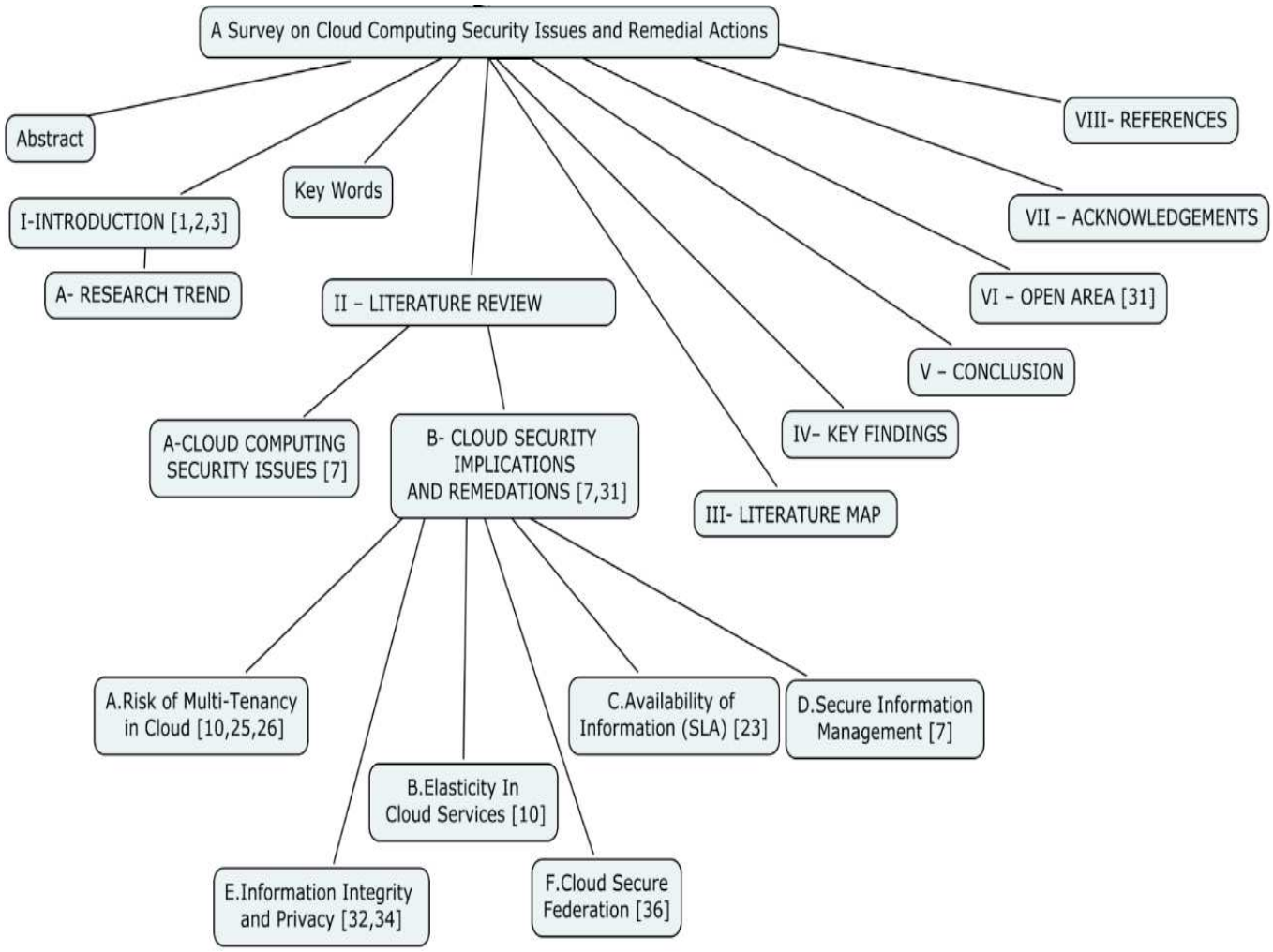


Figure7. Cloud Secure Federation with SSO [37]

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Literature Map



KEY FINDINGS

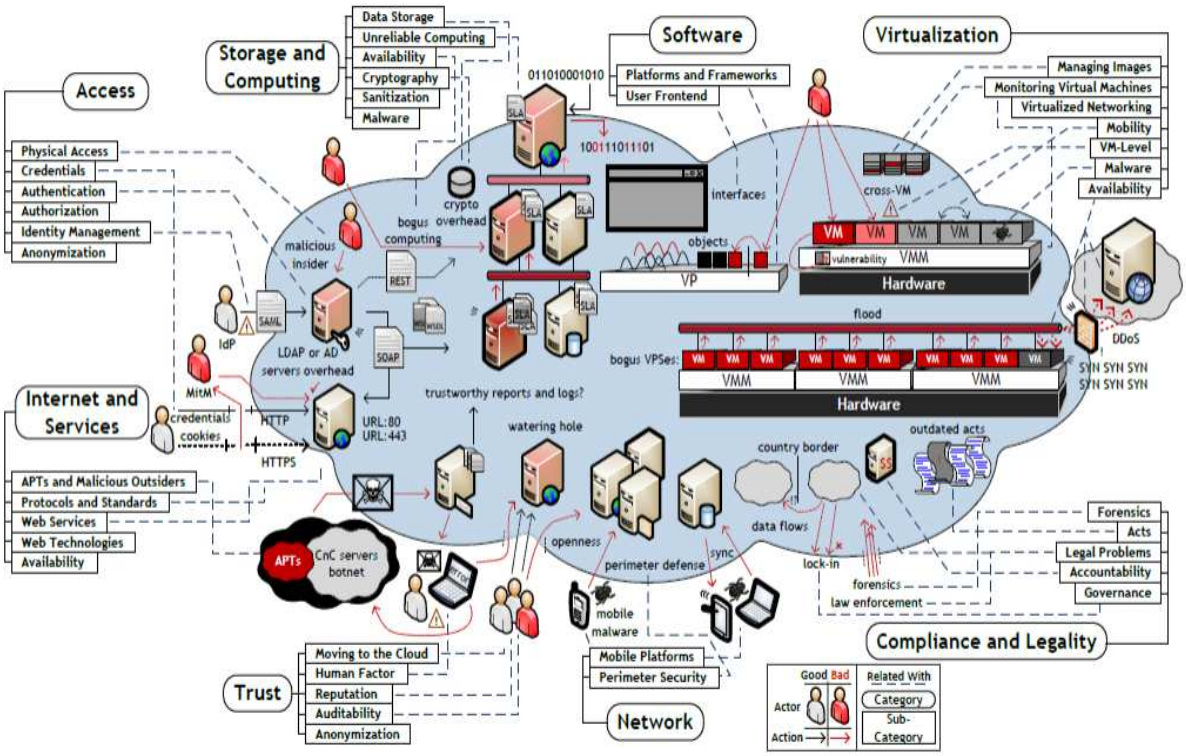
The key findings that we got from the vast literature review that we had mention in the above portion of research paper. We had build an approach or model in our mind by reviewing the vast literature related to the cloud computing world and its available services in the cloud environment [2]. The introduction of cloud computing services Iaas [26],[38] [39] Paas [26], Saas [19] and models which include Public Cloud [40], Private Cloud [41][42], Hybrid Cloud [43]. As well as, the security issues and concerns that arises from the design and architecture in existing services of cloud. Some of the issues developed artificially by humans for using these services in unfair means. Some of the issues that we discussed in the paper which include [7]:

- Risk of Multi-Tenancy in Cloud [10], [25], [26].
- Elasticity in cloud services [10]
- Availability of Information (SLA)
- Secure Information management
- Information Integrity and privacy
- Cloud secure federation

In addition, the solutions or remediation actions for the above prescribed security concerns are also discussed in the survey paper [10], [23], [24], [25], [27], [33], [34], [35], [36], [20]. In addition, machine-learning algorithms are recently being reviewed for cloud computing security [21]. Also a verifiable holomorphic encryption scheme was proposed by a researcher in his paper [22].

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

The intensity level of concerns that shown more critical issue that hesitate IT world for adopting cloud services [22]. We discussed security issues and remedial actions with respect to various cloud providers. The focus of our survey paper is totally dependent on discussing solutions related for cloud computing security issues. For that sake, we have shown a figure that reflects the approach or model that make in our mind from the vast literature review that we have done in the upper portion of survey paper. We have tried to sum up the picture of cloud computing scenario with respect



to their services, appropriate models and issues or flaws that existed in cloud environment. Also, by introduce technical terms that use in cloud computing services and in basic architecture. We also highlight the basic sub techniques or methods that existed in the main nutrients of cloud computing. Moreover, it gives a broad picture related to the concept of cloud environment. As we show this picture to summarize the literature review of the survey paper in a visualization manner. So, even can a lay man having basic concepts of cloud environment should be also able to understand the phenomena that happened in cloud, which is our objective for writing this survey. Figure 8, showing broad picture related to the concepts of cloud environment services and constraints [3].

Conclusion

After the literature review we have concluded that the importance of cloud computing is increasing day by day and drive the IT world for adopting it. Cloud environment is going to be the fifth need of an IT organization after water, electricity, gas and phone grids. It concluded that cloud computing gaining importance because of its facility of use according to demand and pay as peruse which cut downs the cost of IT organizations. Since it is a new technology that still needed to resolve the security issues to win the trust of IT world which encourages them to adopt the cloud environment. There are many security issues that exist in cloud technology but we only focused on the critical ones that must be addressed before the implementation of cloud environment or using the cloud technology with user perspective which

includes multi tenancy, elasticity, availability of information (SLA), secure information management, information integrity, privacy, and cloud secure federation. As cloud computing is one of the promising technologies that facilitates its users more than the previously used grid, distributed and parallel computing. We have to eliminate the existing security issues to make it more convenient. Some of the security issues that had already from the basis of cloud computing which include virtualization. There

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

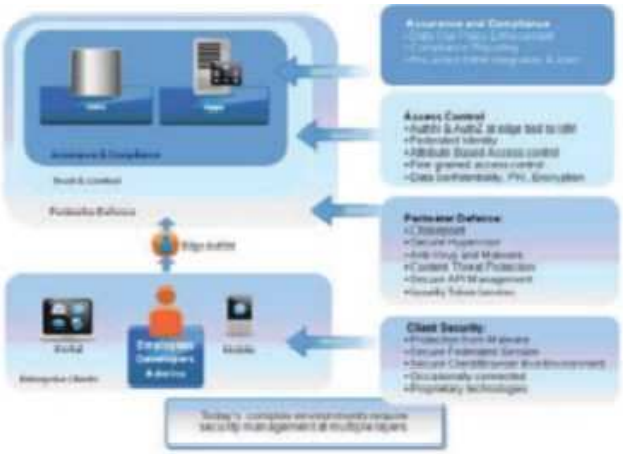


Figure 9. Cloud security wrapper [44]

is a approach define in the form of cloud security wrapper, that provides the multilevel security for accessing the user account. Therefore, it is recommended that cloud computing remedial actions should facilitate the users and organizations for building the trust between them. Nowadays, Cloud computing these days is overwhelmed by an enormous number of difficulties. Because of its fast development and being virtualization is a generally new innovation, an explosion of security issues has been found and concentrated by both the scholarly world and industry.

There is an overall concern encompassing the appropriation of cloud related items. To achieve the target of conveying secure cloud conditions, fixing those security issues is a need. Also, cybercriminals follow patterns, and distributed computing surely doesn't get away from that course. Cybercrime is getting more complex. Malignant entertainers group up and structure malware sequential construction systems, on which everyone has a particular undertaking, such as composing the malware, characterizing spam strategies, plan a social designing segment, and so on. The enterprise network security is presently under exceptionally unpredictable conditions, and the security scene gets more obscure when stirring up cloud conditions with the pace of the expanding and improved digital culpability.

I. VI- OPEN AREA

This research paper has gathered the mainstream issues of cloud computing technology in an easy and simple understanding manner. On other hand it is to facilitate the researchers to further work on the gathering of unresolved issues of cloud computing with respect to (Vendors, Developers, cloud providers, IT organizations, Trouble shooters or anti hackers). That would facilitate in improvising the cloud services and enhancing the security of cloud environment. Therefore, it is still an open field for researchers for future directions. For doing research in this domain, the further improvisation in security of cloud services is one of the best parameter in our opinion. Next, the enlarged Internet traffic and availability exemptions for big business applications and administrations took into consideration more perilous security dangers to show up, as vindictive pages facilitating malware. At long last, the most recent pounding factors are APTs and cell phones that can without much of a stretch jump from inside Wi-Fi net-attempts to radio-based transporter broadband organizations (e.g., 2G, 3G, 4G and 5G). Assembling it each of an invalidated trust model is delivered. People are the source for all these issues and do plan and work to meet their own requirements, yet then the outcome is flawed in some perspective and people endeavour to fill the holes. In any case, that may expect admittance to a heap of resources. In a server centre, there are an incredible number of production resources that should be effectively kept up which could lead an issue since human blunder or carelessness is destined to occur.

References

[1] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." *Future Generation computer systems* 28, no. 3 (2012): 583-592.

[2] Xu, Xun. "From cloud computing to cloud manufacturing." *Robotics and computer-integrated manufacturing* 28, no. 1 (2012): 75-86.

[3] Ruan, Keyun, Joe Carthy, Tahar Kechadi, and Ibrahim Baggili. "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results." *Digital Investigation* 10, no. 1 (2013): 34-43.

[4] Buyya, Rajkumar, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility." *Future Generation computer systems* 25, no. 6 (2009): 599-616.

[5] Avram, Maricela-Georgiana. "Advantages and challenges of adopting cloud computing from an enterprise perspective." *Procedia Technology* 12, no. 0 (2014): 529-534.

[6] Dinh, Hoang T., Chonho Lee, Dusit Niyato, and Ping Wang. "A survey of mobile cloud computing: architecture, applications, and approaches." *Wireless communications and mobile computing* 13, no. 18 (2013): 1587-1611.

[7] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." *International Journal of Information Security and Privacy (IJISP)* 4, no. 2 (2010): 36-48.

[8] Tianfield, Huaglory. "Security issues in cloud computing." In *2012 IEEE International*

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Conference on Systems, Man, and Cybernetics (SMC), pp. 1082-1089. IEEE, 2012.

[9] Chow, Richard, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. "Controlling data in the cloud: outsourcing computation without outsourcing control." In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 85-90. 2009.

[10] Jasti, Amarnath, Payal Shah, Rajeev Nagaraj, and Ravi Pendse. "Security in multi-tenancy cloud." In *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, pp. 35-41. IEEE, 2010.

[11] Alhamad, Mohammed, Tharam Dillon, and Elizabeth Chang. "Conceptual SLA framework for cloud computing." In *4th IEEE International Conference on Digital Ecosystems and Technologies*, pp. 606-610. IEEE, 2010.

[12] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34, no. 1 (2011): 1-11.

[13] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." In *2012 International Conference on Computer Science and Electronics Engineering*, vol. 1, pp. 647-651. IEEE, 2012.

[14] De Donno, Michele, Alberto Giaretta, Nicola Dragoni, Antonio Bucchiarone, and Manuel Mazzara. "Cyber-storms come from clouds: Security of cloud computing in the IoT era." *Future Internet* 11, no. 6 (2019): 127.

[15] Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions." *The Journal of Supercomputing* (2020): 1-40.

[16] Halabi, Talal, and Martine Bellaiche. "A broker-based framework for standardization and management of Cloud Security-SLAs." *Computers & Security* 75 (2018): 59-71.

[17] Vurukonda, Naresh, and B. Thirumala Rao. "A study on data storage security issues in cloud computing." *Procedia Computer Science* 92 (2016): 128-135.

[18] Ismail, Umar Mukhtar, and Shareeful Islam. "A unified framework for cloud security transparency and audit." *Journal of Information Security and Applications* 54 (2020): 102594.

[19] Venkatakotireddy, G., B. Thirumala Rao, and Naresh Vurukonda. "A Review on Security Issue in Security Model of Cloud Computing Environment." In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, pp. 207-212. Springer, Singapore, 2018.

[20] Deshpande, Prachi, S. C. Sharma, Sateesh K. Peddoju, and Ajith Abraham. "Security and service assurance issues in Cloud environment." *International Journal of System Assurance Engineering and Management* 9, no. 1 (2018): 194-207.

[21] Butt, Umer Ahmed, Muhammad Mehmood, Syed Bilal Hussain Shah, Rashid Amin, M. Waqas Shaukat, Syed Mohsan Raza, Doug Young Suh, and Md Piran. "A Review of Machine Learning Algorithms for Cloud Computing Security." *Electronics* 9, no. 9 (2020): 1379.

[22] El-Yahyaoui, Ahmed, and Mohamed Dafir ECH-CHERIF EL KETTANI. "A verifiable fully homomorphic encryption scheme for cloud computing security." *Technologies* 7, no. 1 (2019): 21.

[23] Subramanian, Nalini, and Andrews Jeyaraj. "Recent security challenges in cloud computing." *Computers & Electrical Engineering* 71 (2018): 28-42.

[24] Singh, Saurabh, Young-Sik Jeong, and Jong Hyuk Park. "A survey on cloud computing security: Issues, threats, and solutions." *Journal of Network and Computer Applications* 75 (2016): 200-222.

[25] Alhenaki, Lubna, Alaa Alwatban, Bashaer Alahmri, and Noof Alarifi. "Security in cloud computing: a survey." *International Journal of Computer Science and Information Security (IJCSIS)* 17, no. 4 (2019).

[26] Srivastava, Priyanshu, and Rizwan Khan. "A review paper on cloud computing." *International Journals of Advanced Research in Computer Science and Software Engineering* 8, no. 6 (2018): 17-20.

[27] Gonzalez, Nelson, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Näslund, and Makan Pourzandi. "A quantitative analysis of current security concerns and solutions for cloud computing." *Journal of Cloud Computing: Advances, Systems and Applications* 1, no. 1 (2012): 11.

[28] Kumar, Rakesh, and Rinkaj Goyal. "Assurance of data security and privacy in the cloud: A three-dimensional perspective." *Software Quality Professional* 21, no. 2 (2019): 7-26.

[29] Ordóñez-Morales, Esteban Fernando, Martín López-Nores, Yolanda Blanco-Fernández, Efren Patricio Reinoso-Mendoza, Jack Fernando Bravo-Torres, José Víctor Saiáns-Vázquez, José Juan Pazos-Arias, Manuel Ramos-Cabrer, and Alberto Gil-Solla. "Sporadic cloud-based mobile augmentation on the top of a virtualization Layer: A case

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

study of collaborative downloads in VANETs." *Journal of Advanced Transportation* 2019 (2019).

[30] Afgan, Enis, Andrew Lonie, James Taylor, and Nuwan Goonasekera. "CloudLaunch: discover and deploy cloud applications." *Future Generation Computer Systems* 94 (2019): 802-810.

[31] Taylor, Simon JE, Tamas Kiss, Anastasia Anagnostou, Gabor Terstyanszky, Peter Kacsuk, Joris Costes, and Nicola Fantini. "The CloudSME simulation platform and its applications: A generic multi-cloud platform for developing and executing commercial cloud-based simulations." *Future Generation Computer Systems* 88 (2018): 524-539.

[32] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34, no. 1 (2011): 1-11.

[33] Mastroeni, Loretta, Alessandro Mazzoccoli, and Maurizio Naldi. "Service Level Agreement Violations in Cloud Storage: Insurance and Compensation Sustainability." *Future Internet* 11, no. 7 (2019): 142.

[34] Varshapriya, J. N. "Vulnerabilities, Threats, Attacks in Cloud Computing." *Journal of the Gujarat Research Society* 21, no. 6 (2019): 162-173.

[35] Sengupta, Shubhashis, Vikrant Kaulgud, and Vibhu Saujanya Sharma. "Cloud computing security--trends and research directions." In *2011 IEEE World Congress on Services*, pp. 524-531. IEEE, 2011.

[36] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." *Future Generation computer systems* 28, no. 3 (2012): 583-592.

[37] Celesti, Antonio, Francesco Tusa, Massimo Villari, and Antonio Puliafito. "Three-phase cross-cloud federation model: The cloud sso authentication." In *2010 Second International Conference on Advances in Future Internet*, pp. 94-101. IEEE, 2010.

[38] Manvi, Sunilkumar S., and Gopal Krishna Shyam. "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey." *Journal of network and computer applications* 41 (2014): 424-440.

[39] Gonzales, Dan, Jeremy M. Kaplan, Evan Saltzman, Zev Winkelman, and Dulani Woods. "Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds." *IEEE Transactions on Cloud Computing* 5, no. 3 (2015): 523-536.

[40] Mukundha, Chinthagunta, and K. Vidyamadhuri. "Cloud computing models: a survey." *Adv. Comput. Sci. Technol.* 10, no. 5 (2017): 747-761.

[41] Xiaoning, Li, Li Lei, Jin Lianwen, and Li Desheng. "Constructing a Private Cloud Computing Platform Based on OpenStack [J]." *Telecommunications Science* 9 (2012).

[42] Suciu, George, Elena G. Ularu, and Razvan Craciunescu. "Public versus private cloud adoption—A case study based on open source cloud platforms." In *2012 20th Telecommunications Forum (TELFOR)*, pp. 494-497. IEEE, 2012.

[43] Li, Jin, Yan Kit Li, Xiaofeng Chen, Patrick PC Lee, and Wenjing Lou. "A hybrid cloud approach for secure authorized deduplication." *IEEE Transactions on Parallel and Distributed Systems* 26, no. 5 (2014): 1206-1216.

[44] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." *arXiv preprint arXiv:1609.01107* (2016).

[45] Beimborn, Daniel, Thomas Miletzki, and Stefan Wenzel. "Platform as a service (PaaS)." *Business & Information Systems Engineering* 3, no. 6 (2011): 381-384.

[46] Ali, S. R. (2020). The pattern, sources, and growth of remittances to Pakistan: The kinked exponential approach. Journal of Research in Emerging Markets, 2(1), 1–6. https://doi.org/10.30585/jrems.v2i1.383

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731