Volume: 10 Issue: 06 Pages: 4113-4119 (2019) ISSN: 0975-0290

Cloud Migration: Standards and Regulatory Issues with Their Possible Solutions

Riyaz Ahmad Khan
School of Information Science and Technology, Southwest Jiaotong University, Chengdu-611756, P.R. China
Email: riyaz@my.swjtu.edu.cn
Tianrui Li, Senior Member, IEEE
School of Information Science and Technology, Southwest Jiaotong University, Chengdu-611756, P.R. China
Email: trli@swjtu.edu.cn
Asif Khan
UESTC, Chengdu 611731, China. Crescent University, Chennai 600048, India.
Email: asifkhan@crescent.education

ABSTRACT

To prevent the problem of piracy, cloud computing has become an emerging field to attract enterprises. Most of the organizations (like Amazon, Ramco, Infosys, IBM etc.) are providing their services through cloud computing. These services may be either IaaS or SaaS or PaaS. Even from technological and financial point of view, it is beneficial and may be seductive for the e-commerce companies as well as the customers. There may be several factors at the level of their security, privacy, cost and quality. During migration to Cloud, the consumers as well as companies faces many technological and legislative issues like Cloud Standards, Legislation and Regulatory Issues of CSPs, Security Issues. The objective of this proposal is to mitigate the raised issues between the cloud service provider and the client side in the cloud migration and to propose their effective solutions.
Keywords - **Cloud Computing, Cloud Service Providers, Cloud Standards, E-commerce, Security Issues.**

Date of Submission: April 8, 2019 Date of Acceptance: May 09, 2019

I. INTRODUCTION

Cloud computing, which is a buzzword nowadays gets its name from the drawings typically used to describe the Internet. The concept of cloud computing represents a shift in thought, in those end users need not know the details of a specific technology. Cloud Computing is rapidly growing into many industries at present scenario. For instance, there has been a new trend for e-commerce companies and consumers to adopt Cloud Computing. Most organizations are attracted by Cloud Computing because Cloud can save time and money for them in investing in IT infrastructure. There is no doubt that this may be the biggest benefit brought by Cloud Computing, but Cloud Computing also brings a number of other benefits.

1.1 Why Cloud?

There are many questions that arise as to whether a cloud is need of time at present. Whether Cloud is reliable, easily adoptable and suitable for all the consumers and the e-commerce companies [1]. Cloud Computing gets more and more popular as it can be applied nearly everywhere: the libraries, the fire services, the small retailers which need secure e-commerce websites. When talking about beneficiaries of Cloud Computing, people always think of Cloud consumers. Actually, not only Cloud consumers including the organizations and end-users, but also Cloud providers can benefit from it.

1.1.1 Benefits for Cloud providers

There are several benefits for organizations to provide Cloud services.

- **Make Money:** Profit is always the most attractive thing for business people. And a large company acts as a Cloud provider could make a tidy profit when they leverage their economies of scale to offer a service.
- **Leverage Existing Investment:** Using existing idle IT infrastructure to provide Cloud service enable companies to have a new revenue stream. For example, Amazon and Google extended their private Clouds and offered to the public.
- **Defend a Franchise:** Since many of enterprise applications begin to make use of Cloud Computing, vendors would be motivated to provide a Cloud option of their own if they already established franchise Cloud Computing in E-commerce in those applications.
- **Leverage Customer Relationship:** Companies can get extensive customer relationship via their service offerings, including Cloud service.

1.1.2 Benefits for Cloud consumers

Here, the Cloud consumers refer to companies and organizations that adopt Cloud Computing. Armbrust et al. gave reasons to explain why these organizations want to move to Cloud.

- **Pay as Used:** Small companies do not need to invest in the initial IT infrastructure and maintain them if they adopt cloud. They can simply pay as they used. In this way, companies can reduce the waste of underutilization.

Volume: 10 Issue: 06 Pages: 4113-4119 (2019) ISSN: 0975-0290

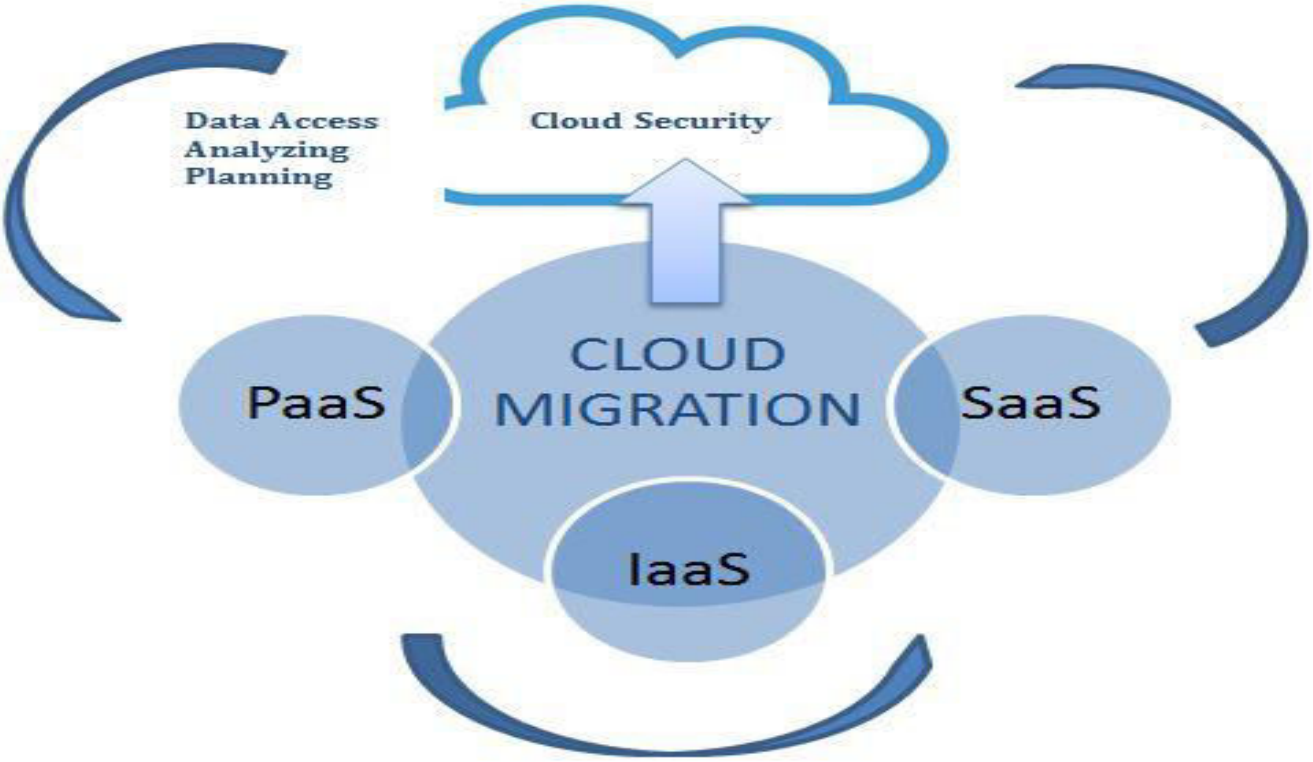

Figure 1. Cloud Security Flow Process

 Reduce Operation Cost: Since Utility Computing uses virtual machine instead of physical machine; the work virtual machine instead of physical machine; the work of hardware operation is shifted from Cloud consumers to Cloud providers. Organizations can reduce their operation cost in this way.

1.1.3 Benefits for end-users

End-users of Cloud service actually are the most important users. For the end-users of Cloud Computing, the incentives are similar to those motivating enterprises and organizations [23]. They require easy-to-use interfaces, appropriately reliable and timely service delivery, information about their services, etc. With Cloud Computing, end-users can access and update information wherever they are, rather than having to run back to their offices [18]. Moreover, Cloud Computing accomplishes a better response time than standard server and hardware in most cases

I. RELATED WORK

Cloud Models: There is no doubt that Cloud works for many use cases, but, not all the Cloud is the same. There are three principal ways Cloud services can be delivered: public Cloud, private Cloud and hybrid Cloud.

 Public Cloud: A public Cloud is a service delivery model which provides massively scalable IT resources available to the general public through the Internet. It is usually based on a usage-based model. Amazon EC2, Google App Engine and Force.com are the best known examples of public Cloud service providers [20]. It sounds like public Cloud is a good choice for the companies, especially for the small companies as they do not need to invest too much on the IT infrastructures. But the truth is, many organizations hesitate to use public Cloud due to security issues.

 Private Cloud: In contrast, private Cloud represents a deployment model that offer Cloud service to the internal users within the corporate network. It is relatively secure compare with public Cloud. But meanwhile, it brings another problem: capital to build private Cloud.

 Hybrid Cloud: Hybrid Cloud is a composition of public and private Cloud. Organizations provide and manage some resources in-house and at the same time, have others provided externally. It allows a business to take advantages both of public Cloud and private Cloud. Thus, hybrid Cloud is considered as the next wave in Cloud Computing.

Cloud computing models can be broken into three basic designs, which are described below:

Infrastructure as a Service: As the name implies, you are buying infrastructure. This refers to computing resources as a service. The resource could be virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access [27]. You own the software and are purchasing virtual power to execute as needed. This is much like running a virtual server on your own equipment, except you are now running a virtual server on a virtual disk. This model is similar to a utility company model, as you pay for what you use.

Volume: 10 Issue: 06 Pages: 4113-4119 (2019) ISSN: 0975-0290

Platform as a Service: In this model of cloud computing, the provider provides a platform for your use. Services provided by this model include all phases of the System Development Life Cycle (SDLC) and can use Application Program Interfaces (APIs), website portals, or gateway software. Buyers do need to look closely at specific solutions, because some providers do not allow software created by their customers to be moved off the provider's platform. This can be thought as IaaS with a custom software stack for the given application [17]. But the difference between them is PaaS also includes operating systems and required services for a particular application.

Software as a Service: This model is designed to provide everything and simply rent out the software to the user. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a per use fee. All work that has been done will save in cloud, end user starts from where he/she stopped working. This is based on licensing software use on demand that is installed and running on a Cloud platform already [19]. It reduces the user's physical equipment deployment and management cost. In addition, SaaS also allows users to compose their existing services to meet their requirements.

II. ISSUES TO CONSIDER PRIOR TO CLOUD ADOPTION

3.1 Security

Security of data in public Clouds is a big concern. Although CSPs always say that the information of clients are stored securely on the Cloud. But e-commerce companies and Cloud end-users still worry about the security of their data since their sensitive data are in the hands of Cloud Service Providers [26]. Since both Cloud Computing and e-commerce have security problems, this issue may be the most serious one that makes customers hesitate to implement Cloud e-commerce. Customers are concerning about security because they feel they lose control of their data, and most of them do not have the experience of using Cloud before. As this report stated before, e-commerce and consumers have several security issues [16]. However, after e-commerce moving to the Cloud, all of the e-commerce activities would be done on Cloud. The security of Cloud will be the most urgent one to be noticed [29]. Before moving to Cloud Computing, Foster et al. suggested to discuss following issues with vendors in terms of security.

 Privileged User Access: The sensitive data that processed outside the enterprise need to be assured that they are only accessible to privileged users.

 Regulatory Compliance: Cloud consumers must verify if a Cloud provider has external audits and security certifications. And, they need to know if their infrastructure complies with some regulatory security requirements.

 Data Location: It is important that the Cloud providers commit to storing and processing data in specific jurisdictions since customers will not know where their data will be stored.

 Data Segregation: One customer's data must be fully segregated from another customer's data.

 Recovery: Cloud customers must ensure their Cloud provider has an efficient replication and recovery mechanism to restore data.

 Investigate Support: Cloud service is difficult to investigate. Such support needs to be ensured if it is important for a customer.

 Long-term Viability: Cloud customer must assure their data would be viable even their Cloud provider is acquired by another company.

3.2 Privacy Protection: Cloud Computing is normally based on the existing distribute network. Computers can be a part of Cloud as soon as they connect to the Internet. E-commerce activities require customers 'personal information, such as name, address, identity, bank data, etc. Attackers can attack the individual privacy by using multiple links between data if there is no believable privacy [28]. For example, Sony announced that hackers have stolen Sony Online Entertainment (SOE) customer information which was stored on their private Cloud in May, 2011. There are approximately 24.6 million SOE accounts may have been stolen [14]. The illegally obtained information includes customer's names, addresses, e-mail addresses, birthdates, genders, phone numbers, login names and hashed passwords. Cloud providers must try to safeguard their customer's privacy [25]. Particularly, it is essential for the adoption of public Cloud systems that customers are reassured that security and privacy is not compromised.

3.3 Cost

Profit is always the most important objective which business people are pursuing. Cloud Computing is attractive as it can save them millions of dollars to build their own servers and storage environment. The cost of Cloud service matters a lot to e-commerce companies and other consumers. At present, price of Cloud service is relatively low. Cloud service providers, such as Google and Amazon, are trying to make the price more transparent to customers. They also make efforts to enhance their competitiveness by reducing their service cost [21]. There is a series of cost for using Cloud Computing. Enterprises pay for the Total Cost of Ownership (TOC) which is calculated from the pricing models of Cloud providers. Software development cost, integration and customization cost, subscription cost (for SaaS Clouds), hardware and middleware cost, data IO transfer cost, etc. are covered in TCO [4]. Organizations need to estimate Cloud Computing costs and compare these costs with conventional IT solutions. Cost and benefit analysis is important for an IT managers to evaluate whether the benefits outweighs the costs of an IT investments. Different execution plans may result in significantly different costs. Hence, to have a precise estimate and plan of usage will reduce the cost of adopting Cloud.

Volume: 10 Issue: 06 Pages: 4113-4119 (2019) ISSN: 0975-0290

3.4 Quality

The Quality of Service (QoS) is a broad topic in distributed system. It is mostly referred to the resource reservation control mechanism to guarantee a certain level of performance and availability of a service. It is a crucial factor for the success of Cloud providers as it may destroy a provider‘s reputation [24]. Computing services need to be highly reliable, scalable, and autonomic to support ubiquitous access, composability and dynamic discovery. Cloud service providers such as Amazon, Google, IBM, Microsoft and Sales force have established their data centers for hosting Cloud applications in various locations around the world in order to provide redundancy and ensure reliability in case of site failures. SLAs assure end-users that they are receiving the services they have paid for by providing a facility to agree upon QoS between end-users and providers and define end-user resource requirements and provider guarantees [2]. It typically includes error rate, max response time and throughput. Also, it may include non-functional requirements such as scalability, availability. In the past few years, crashes of Cloud servers took place frequently. The interruptions of Cloud service have had negative effects among users. Cloud service providers need to improve their service quality to enhance the confidence of users to use their Cloud services. Before purchasing Cloud service, to sign a SLA is essential for consumers [7], [8]. The success of adopting Cloud Computing depends largely on the service quality provided by Cloud provider. Hopefully, more advanced and customizable SLAs are being supported or implemented.

III. MIGRATION

The above four factors security, privacy, cost and quality are the issues which all consumers and e-commerce companies should consider about before moving to Cloud as shown in figure 1. For companies which already have their own infrastructure, they should think about migration effort [12]. This effort is due to the discrepancies between the environment provided by a Cloud platform and a traditional platform. In other words, there might be differences in the version of various infrastructures, the libraries available, the programming models, even the semantics of data access [3], [5].

The following are the factors relevant to migration to Cloud.

 Existing knowledge and experience on Cloud providers and technologies: If the project team already have some prior knowledge and experiences of Cloud and available tools, less effort is required since the learning curve can be improved significantly.

 Selecting the correct Cloud platforms and services (IaaS or PaaS): This factor affects the effort and cost required for the rest of migration activities greatly as shown in figure 1. Less effort is required for modification if the selected Cloud platform is highly similar to the application‘s environment in the local server.

 Compatibility Issues: This factor is affected by the similarity of Cloud platforms and local servers as well. Compatibility issues can be eliminated when the similarity is high [15].

 Library Dependency: If an application relies on a library to function in local server, it requires a similar library in the Cloud platform [13]. Thus, if there is such a library for Cloud existing, less effort would be required to rewrite that library. Contextualization mechanism, which is proposed by Armstrong et al., could help to save the effort of rewrite the library. The mechanism operates in two stages. The first stage contextualization of VM images is prior to service deployment (PaaS level). This stage involves mounting a template VM image which will be converted to a specific hypervisor and installing proper software packages to support a particular service, such as a database. In this stage, context data is generated for every envisaged VM instance as an ISO CD image. The second is self-contextualization of VM instances created from such a VM image (IaaS level). During this stage, entails reading in context data at run time when the VM image is instantiated [6]. Then the data will be used to configure the installed packages and software in the VM image. Then a single image will be able to spawn multiple instances of the same software component forming a multi-VM service [22], [30].

 Connection Issues: In the Cloud migration cases that only some components of the system are migrated to Cloud while the rest is kept in house, the connection between two parts of the system (one in house and the other one in Cloud) may face different issues such as security, latency, etc. Moreover, the companies which already have their own existing facilities should consider one more factors in migration cost [9]. They cannot avoid the additional costs for giving up their established infrastructures. There will be a trade-off when making decisions. If an e-commerce company wants to move to Cloud from their existing infrastructure, they must have a complete plan of migration as discussed in figure 1. Otherwise, they may encounter some unexpected difficulties in the adoption of Cloud.

IV. ISSUES THAT NEED TO BE SOLVED AND THEIR PROPOSED SOLUTION

5.1 Cloud Standards

Because your data is in the cloud, you may not realize that the data must reside in a physical location. Standardized options and solutions for Cloud which include assurance, provision of trust and frameworks including associated APIs to expose what Cloud service providers are doing, are currently missing. There is no standard for how data is stored, performance metrics or access controls. The lack of standards also makes it impossible for Cloud consumers to identify the level of security offered by individual CSPs. The discussion for Cloud standards lasts for a long time. Experts in the industry do not hold a positive attitude to the standardization of Cloud Computing. Cloud Computing standards, has not even gone to the first stage, need time to evolve. Steven Dietch, the VP of HP Cloud

Volume: 10 Issue: 06 Pages: 4113-4119 (2019) ISSN: 0975-0290

solutions infrastructure markets said in one of his keynote presentations [10]. At present, many organizations have established their own Cloud platforms and provided Cloud services. And some of them have developed their own standards. Different standards of different platforms cause difficulties for Clouds to communicate. In other words, the interoperability is low. The lacking of Cloud standards impedes the acceptation of Clouds [11]. Users are worrying about data migration between Cloud servers. Furthermore, they are afraid that Cloud service providers may use this flaw to restrict them. It's a valid concern, because if one company relies highly on a CSP, then the CSP increase their service price. The company will face a dilemma since the migration to other Cloud may cost more. They will lose their bargaining power.

Possible Solutions: In order to remove the concerns of potential Cloud consumers, e-commerce companies and pick their interest towards the Clouds on the more reasonable basis, CSPs must provide better and more reasonable standards so that adaptation of the Clouds could be preserved as shown in figure 2. Standards and encryption might be discussed enough. Is it being used while the data is at rest and in transition? Anyone will also want to know what type of standards and encryption is being used. For example, there is a big difference between WEP and WPA2 etc.

Figure 2. Cloud Security Model

5.2 Legislation and Regulatory Issues of CSPs

All the Cloud consumers and the involved e-commerce companies put their data and software on the Cloud; therefore CSPs must take their responsibility to ensure the security of the information. Organizations operating in the US, Canada, or the European Union have many regulatory requirements that they must abide by. For example ISO 27002, Safe Harbor, ITIL, and COBIT. You must ensure that your cloud provider is able to meet these requirements and is willing to undergo certification, accreditation, and review. But, how to supervise the operations and standardize the services is a problem that needs to be solved. At present, there are no corresponding laws and regulations for Cloud e-commerce. The lack of legislation may cause some problems in practice and the concerned companies and the all of the consumers may hesitate to be involved over there.

Possible Solution: There should be an existence of CSPs Council and a CSPs Regulation Act. This should not be control but regulated as shown in figure 2. The difference between the two ways is, in control there is no freedom, but in regulation there is freedom but it is subjected to reasonable restrictions as being the public interest, consumers or companies. And it should not be regulated by the government, but by an independent regulatory authority supposedly the CSPs council. There should be a fixed number of members of the CSPs council. Out of some are representative of the CSPs council. And some of them are appointed by the government, are elected by the CSPs organization. So all the decisions are taken by majority votes. No one can be dictator that imposed his views on CSPs Council. Sometimes his suggestions are accepted by the CSPs Council, sometimes rejected so that respects to the verdicts of majority. CSPs Council should not wholly appointed by government. But they should be appointed by their pupil as shown in figure 2. They themselves should elect their representatives by their organizations. But it should be a statutory body, not the kind of private body. They should be deciding themselves, but their body must have power to suspend the license if anyone not ethically fit for this profession.

V. CONCLUSION

The benefits of cloud computing are many. One is reduced cost, since you pay as you go. Other benefits are the portability of the application is that users can work from home, work, or at client locations. This increased mobility means employees can access information anywhere they are. There is also the ability of cloud computing to free-up IT workers who may have been occupied performing updates, installing patches, or providing application support.

While cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater level of security than the organization would have if the cloud were not used. There should be a regulatory body that has legislative power to ensure the integrity and security of cloud systems and should be able to punish the adversary or the culprits when needed.

Volume: 10 Issue: 06 Pages: 4113-4119 (2019) ISSN: 0975-0290

ACKNOWLEDGEMENTS
The Key lab of Cloud Computing, SWJTU, China.

REFERENCES

[1] R. Hopkins and K. Jenkins, *Eating the IT Elephant: Moving from Greenfield Development to Brownfield* (IBM Press, 2008).

[2] R. Khajeh-Hosseini, A., Sommerville, I., Bogaerts, J., & Teregowda, P. (2011, July). Decision support tools for cloud migration in the enterprise. In Cloud Computing (CLOUD) *2011 IEEE International Conference on* (pp. 541-548). IEEE 2011.

[3] Dawoud, W., Takouna, I., Meinel, C. Infrastructure as a service security: Challenges and solutions. Informatics and Systems (INFOS), *The 7th International Conference*, pp.1-8, 28-30 March 2010.

[4] Singh H, A. P. S. N. Campus. Technology transfer model to migrate e-governance to cloud computing. IJATER (Int J Adv Technol Eng Res) 2012; 2(4):52-7.

[5] Syed Hamid Hussain Madni, Muhammad Shafie Abd Latiff, Yahaya Coulibaly and Shafi'i Muhammad Abdulhamid, Resource Scheduling for Infrastructure as a Service (IaaS) in Cloud Computing: Challenges and Opportunities, *Journal of Network and Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2016.04.016

[6] Conway G, Curry E. Managing cloud computing-A life cycle approach. CLOSER; 2012. p. 198-207.

[7] Khajeh-Hosseini A, Greenwood D, Smith JW, Sommerville I. The cloud adoption toolkit: supporting cloud adoption decisions in the enterprise. *Software Pract Exp* 2012;42(4):447-65.

[8] A Khan, S Deep, JP Li, K Kumar, RA Shaikh, F Hasan, *2014 11th International Computer Conference on Wavelet Actiev Media Technology and Information Processing* (ICCWAMTIP) Pages 293-296.

[9] Nasr AO, Galal-Edeen GH. Proposed development model of e-government to appropriate cloud computing. Int J Rev Comput 2012; 9(7):1-7.

[10] Taher Y, Haque R, Nquyen DK, Van den Heuvel WJ. Designing and delivering public services on the cloud. In: *International conference on cloud computing and services science*; 2011.

[11] Trivedi H. *Cloud computing adoption model for governments and large enterprises* [Doctoral dissertation]. Massachusetts Institute of Technology; 2013.

[12] Singh VJ, Chandel A. Evolving e-governance through cloud computing based environment. *Int J Adv Res Comput Commun Eng* 2014;3(4):6188-91.

[13] Maluleka SM, Ruxwana N. A framework for cloud computing adoption in South African government: a case of department of social development. In: *Proceedings of international conference on business management & IS*, vol. 2; 2013. No. 1.

[14] Veljanovska K, Zdravevska V. E-government based on cloud computing. J Emerg Trends Comput Inf Sci 2013;4:377-81.

[15] Badger L, Bernstein D, Bohn R, De Vaulx F, Hogan M, Iorga M, et al. US government cloud computing technology roadmap, vol. I. National Institute of Standards and Technology; 2014. https://doi.org/10.6028/ NIST.SP.500-293.

[16] Alshomrani S, Qamar S. Cloud based e-government: benefits and challenges. *Int J Multidiscip Sci Eng* 2013;4(6):1-7.

[17] Kundra V. Federal cloud computing strategy. 2011.

[18] Varma V. Cloud computing for E-governance. A White Paper IIIT Hyderabad; 2010. http://www.iiit.ac.in/~vasu.

[19] Hashemi S, Monfaredi K, Masdari M. Using cloud computing for egovernment: challenges and benefits, "World Academy of Science, Engineering and Technology, international science index 81. *Int J Inf Sci Eng* 2013;7(9):987-95.

[20] Almarabeh T, Majdalawi YK, Mohammad H. Cloud computing of egovernment. Commun Netw 2016;8(1):1.

[21] Craig R, Frazier J, Jacknis N, Murphy S, Purcell C, Spencer P, et al. Cloud computing in the public sector," Public manager's guide to evaluating and adopting cloud computing. White Paper. Cisco Internet Business Solutions Group; 2009.

[22] Kumar P, Kumar D, Kumar N. Improved service delivery and cost effective framework for e-governance in India. 2013.

[23] C.Carvalho, R.M. Andrade, M.F De Castro, E. Coutinho, N.Agoulmine, State of the art and challenges of security SLA for cloud computing. Computers and Electrical Engineering 000 (2017) 1–12. http://dx.doi.org/10.1016/j.compeleceng.2016.12.030

[24] Perez-Botero D, Szefer J, Lee RB. Characterizing hypervisor vulnerabilities in cloud computing servers. In *Proc. of the 2013 international workshop*

Volume: 10 Issue: 06 Pages: 4113-4119 (2019) ISSN: 0975-0290

on Security in cloud computing 2013 May 8 (pp. 3-10). ACM.

[25] S. Iqbal, L. Mat Kiah, B. Dhaghighi, M. Hussain, S. khan, M. Khurram Khan, On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service, *Journal of Network and Computer Applications*, http://dx.doi.org/10.1016/j.jnca.2016.08.016

[26] CLOUD SECURITY ALLIANCE, The Treacherous 12 - Cloud Computing Top Threats in 2016.

[27] Saravana Kumar Na, Rajya Lakshmi G.Vb, Balamurugan Ba, Enhanced Attribute Based Encryption for Cloud Computing. *International Conference on Information and Communication Technologies* (ICICT 2014).

[28] S. Subashini, V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* Volume 34, Issue 1, January 2011.

[29] Dale D. Reitze, Using Commercial Web Services to Build Automated Test Equipment Cloud Based Applications, *IEEE* 2014.

[30] Abida Sharif, Jian Ping Li, Muhammad Asim Saleem. Internet of Things Enabled Vehicular and Ad Hoc Networks for Smart City Traffic Monitoring and Controlling: A Review. *Int. J. Advanced Networking and Applications*, Volume: 10 Issue: 03 Pages: 3833-3842 (2018) ISSN: 0975-0290, November 2018.

Biographies

Khan Riyaz Ahmad is Research Scholar in School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China. His interest area covers- Big Data Processing, Cloud Computing, Social Networking, Robotics, Artificial Intelligence and Image Processing related fields. He is also associated with SWJTU-LEEDS Joint School, Southwest Jiaotong University, China; University of Leeds, England, UK.

Tianrui Li (SM'10) received the BS, MS, and PhD degrees from Southwest Jiaotong University, Chengdu, China, in 1992, 1995, and 2002, respectively. He was a postdoctoral researcher with SCK-CEN, Belgium, from 2005 to 2006, and a visiting professor with Hasselt University, Belgium, in 2008, the University of Technology, Sydney, Australia, in 2009, and the University of Regina, Canada, in 2014. He is currently a professor and the director of the Key Laboratory of Cloud Computing and Intelligent Techniques, Southwest Jiaotong University. He has authored or coauthored more than 100 research papers in refereed journals and conferences. His research interests include big data, cloud computing, data mining, granular computing, and rough sets. He is a senior member of the IEEE.

Khan Asif is a Postdoc Research Faculty in School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC) Chengdu, China. Dr. Khan is also associated with Crescent University, Chennai, India. He has done Ph.D. in Computer Science and Technology which was achieved with honors in 2016 and Awarded by UESTC's 'Academic Achievement Award' and' Excellent Performance Award' 2015-16. Mr. Khan is an Adjunct Faculty: University Of Bridgeport, USA for China Program in summer from 2016. Previously he was a visiting scholar for Big data Mining and Application at "Chongqing Institute of Green and Intelligent Technology (CIGIT), Chinese Academy of Sciences", Chongqing, China. His main interests are the robotics vision and new ideas regarding vision based information critical research work in Artificial Inelegancy, Image processing, Computer Vision and social networking based theoretical research.