Science, Engineering & Education, 2, (1), 2017, 41-49

Cloud computing - a review on benefits, challenges and applications

Hieu Vu Tran[1*], Binh T.H. Nguyen[2], Ngoc Dung Bui[1]

[1] Faculty of Information Technology, University of Transport and Communications, Hanoi, Vietnam
[2] Information Technology Department, University of Transport and Communications, HCMC Campus, Ho Chi Minh City, Vietnam

Received 30 September 2017, Accepted 10 November 2017

ABSTRACT

In this paper the applications, benefits and challenges of cloud computing are reviewed. Firstly in 1960s the main concept of cloud computing was given by Professor John McCarthy from Stanford University. He stated that computation and computer's applications will become public utilities. Nowadays, the users can use resources and applications with cloud through Internet. Cloud computing has many superior aspects such as costs, elasticity, resource pooling, self-service information technology infrastructure, service can be measured. Nevertheless there are still some barriers that prevent the development of cloud computing such as availability of service, data lock in, data transfer bottlenecks, reputation fate sharing, software licenses and security. The top security threats of clouds are also mentioned in this paper.

Keywords: Cloud computing, Security, Data transfer, Sharing.

INTRODUCTION

In 1961 Professor John McCarthy affirmed that computation and computer's applications will become public utilities; this is an abstraction of cloud computing [1, 2]. Cloud computing is a new trend of Information technology, which arose in 2007 [3]. According to [1], cloud computing can '… moves computing and data away from desktop and portable PCs into large data centers'. Many computer services can be supplied only with a web browser [4]. And with cloud computing, '… machines in larger data centers can be dynamically provisioned, configured, and reconfigured to deliver services in a scalable manner for needs ranging from scientific research to video sharing to email' based on [5]. With deployment of cloud, many aspects of human being are greatly improved, for example clouds are important factor to enhance development of health care [6 - 8]. Personal health records and health related services can be easily used by patients, doctors and hospitals at any location, this trend also can help to reduce the initial cost for IT infrastructure [6 - 8].

Cloud computing also supports the development of many technologies such as mobile com-

* *Correspondence to: Hieu Vu Tran, Faculty of Information Technology, University of Transport and Communications, No.3 Cau Giay Str., Lang Thuong Ward, Dong Da District, Hanoi, Vietnam, E-mail: hieutv@utc.edu.vn*

puting, IOT. Nowadays, smartphone becomes very popular, many smartphone's applications become important part of the modern life. However smartphone has limited memory, limited battery life, low processing power... and can reduce the effectiveness of the mobile applications. Cloud computing with support of technology solution, named computer offloading, can migrate data processing, data storage... from mobile devices to powerful servers of cloud, and as a result can improve battery life and also can build excellent mobile cloud computing's applications [9 - 11]. According to Othman and his colleagues, there are some types of mobile cloud computing application models: performance based application models which improve the performance using cloud resources, the energy based application models which increase battery life of mobile devices using cloud resources, the constrain based application models, which contain application, can still run in limited resource environment, and the last are multi-object application models which support more than one of three above conditions [10]. The virtualized processing power and unlimited resources of cloud are also can build great solution for IoT [12].

In this report, the benefit and barriers of cloud computing will be mentioned. Firstly this report will show the introductions which include definitions, three service models, deployment models, and the applications of cloud computing. Secondly advantages of cloud computing will be listed: costs, elasticity, resource pooling, self-service information technology infrastructure, service can be measured. But there are still many challenges with cloud computing: availability of service, data lock-in, data transfer bottlenecks, reputation fate sharing, software license and security.

W. Kim et al. [4] indicate that the definition of the cloud contains two parts. The first part is accessing the resources through Internet and the resources which are managed distantly and dynamically allocated and reallocated according to needs of the users', the second part is paying for the actual use of the computing resources. The National Institute of Standards and Technology (NIST), Information Technology Laboratory in United States of American [13] provided a more comprehensive definition: "cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Nowadays "cloud computing is already being used by ten millions of people in various manifestations, including free e-mail services such as Yahoo Mail, Hot Mail, Gmail, etc.; and free office productivity applications, such as Google Apps…"[4]. Three are the service models of cloud computing:

First one is SaaS which means software as a service. With SaaS, instead of storing and working with computer applications in their own laptop or PC, the users can access and work with these applications through Internet. These cloud products are Yahoo mail, Google Apps, Salesforce.com, WebEx, Microsoft office live [14 - 15]. Salesforce.com was created in 1999 by Marc Benioff, who is also one of the first people thinking about supply enterprise applications to customers through simple web browser [2].

Second one is PaaS which means platform as a service and it is the platform to develop new applications in the cloud. With PaaS "… developer can design, build, and test applications that run on cloud provider's infrastructure and then deliver those applications to end users from provider's servers" [15]. The early market leaders are Google's Apps engine, Microsoft's Azure, Amazon Web services, Force.com, Coghead [14 - 15].

Third one is IaaS which stands for infrastructure as a service. IaaS will supply computing, storage, network services and other resources to customers. Miller and Veiga [15] state that "those who buy and use IaaS are predominantly the IT/system administrator types charged with obtaining general processing, storage, database man-

agement, and other course IT resources and applications". Main vendors of IaaS are Amazon's EC2, GoGrid's Cloud Servers, Joyent [14 - 15].

Cloud computing has some deployment models and these models will be applied according to the purposes of the users:

A private cloud is used by only one company and administered by this company or a third-party company [13, 16 - 17]. This model has some advantages, the private cloud can increase the level of security of data privacy and trust [16] and the cost of transfer data "… from local IT infrastructure to a Public Cloud is rather considerable" [16].

A community cloud is used by more than one company and the cloud can be administrated by an arbiter company or one company in the group above [13], [16 - 17].

In public model, cloud will be used by communal users, cloud provider owns entirely a public cloud and makes policies to use the cloud, spend money to keep public cloud working, provide services to users and gain back money [13, 16 - 17].

A hybrid cloud contains more than two clouds with all type above [13, 16 - 17]. With an hybrid cloud, the corporations still can run non important applications in public cloud and important applications and save data in private cloud [17].

Methods

In this part, both practical and academic view of applications of cloud computing, benefits and challenges are given.

Applications of cloud computing

Cloud computing assists cloud providers to become "… the world primary computers" [5] and it is useful not only with individual users, companies but also with governments. Individual users mostly use cloud computing for storing e-mails, other documents and using computer's applications [5]. Besides, Hand's study in 2007 [5] found that "cloud providers already offer a variety of services to individuals, companies, and government agencies, with users employing cloud computing for storing and sharing information, database management and mining, and deploy Web services that can range from processing vast datasets for complicated scientific problems to using clouds to manage and provide access to medical reports". Corporations '…can use the vast computing power available to add new dimension to their current IT infrastructure' as reported on page 246 of [5]. More and more corporations want to implement cloud in large scale [18, 19]. The biggest information technology corporation in the whole world (Microsoft) and Japanese biggest information technology services provider (Fujitsu) '…have agreed on a partnership in global cloud computing, where data and programmes are stored on servers that are accessed online rather than on users' computers' as stated in paragraph 1 of [18]. Fujitsu also starts to use Window Azure in all of their centers from 2010 [18]. Cloud computing can also be used by governments. Chief Technology Officer Vivek Kundra of United States of America states that cloud computing will change way government work [5]. Government of United States of America begun to use cloud computing in 2009 e-government portal USA.gov and this Spanish version GobiernoUSA.gov used cloud computing technology [5].

Benefits of cloud computing

Cloud computing has many fascinating aspects. Some main superiorities of cloud computing that are always be mentioned in research articles are listed below.

Costs

With the traditional way to develop an application service, a huge amount of money (which is called capital expense) will be ordered to invest on building infrastructure for maximum service demand before operating [14]. However, with cloud computing this problem will be solved "…by allowing expenses to track closely with resource use, thus following income rather than

having to purchase for peak capacity before income is realized" [14]. This will move capital expense (CapEx) to operational expense (OpEx) and normally, operational expense like cost for employing new service is much lower than capital expense [14, 20].

When using cloud computing, you will spend money just for what you use [13]. Pay as you go is the model of cloud computing, users only need to pay money rely on the time they use services, capacity of storage or other measurable means in cloud [13]. This will reduce money that users have to spend to use services.

Elasticity

With cloud computing, resources will be very elastic [13, 16 - 17, 21 - 22]. Durkee [21] describes that "computing is provided in the amount required and disposed of when no longer needed". Resources of cloud computing can be easily "… scaled up and down rapidly and elastically" [22]. Because of this advantage, users do not need to worry about up-front commitments or contracts, they can scale up when they want and they can release when they want to scale down [16]. Cloud computing can "….allow matching resources to workload much more closely" [20]. For example, a service desires five hundred servers at noon but it only craves one hundred servers at midnight [20]. With conventional way of using resource, provider of this service must always supply for the highest demand with five hundred servers and will discharge 500 * 24 = 12,000 server-hours [20]. But when using cloud computing, the provider only provisions for average of usage which is three hundred servers [20]. And cost will be 300 * 24 = 7,200 server-hours and it is only 60 % compare to the first option [20]. Moreover in real world, this example still cannot present all advantages of elasticity, because sometimes service does not require as much resources as usual, some example such as electronic commerce in December or sharing photo website after holidays [20], and during this duration of time providers of these services even can save more money.

Resource pooling

Resource pooling is another advantage of cloud computing because "the cloud provider's infrastructure is shared across some number of end customers, providing economies of scale at computing and service layers" [21]. Resources (CPU, database…) from cloud provider will be pooled with homogeneous structure to supply for multiply users [16, 22]. With this strategy, users do not know locations, formation, originalities of the resources, they even cannot answer when someone ask them where cloud provider store their database [16].

Self-service infrastructure

Self-service information technology infrastructure is a very fascinating feature of cloud [14, 16, 22]. Users can demand and manage services without human interaction with service provider. Before existing of cloud computing, non-information technology companies which want to develop an application must contact directly and have some face-to-face meeting with other information technology companies to outsource. People who want to use some resources need to contact directly with the owner of resources [16]. But with cloud computing, they can use web portal, management interface instead of human interaction to contact with the information technology companies or owner of resources [22].

Service can be measured

Another good attribute is that the service can be measured [16, 22]. Although resources are shared between many users, the usage of resources of each user can be measured [16]. Resources are always "…constantly metered, supporting optimization of resource usage, usage reporting to the customer and pay-as-you-go business models" [22].

Challenges of cloud computing

Despite that cloud has many attractive attributes for cloud developers and consumers, there are still many challenges that can prevent customers

and organizations from using cloud computing.

Availability of service

The first problem with cloud computing is availability of service. With giant cloud providers "… maintaining 24/7 up time is crucial to their business…" [5]. If outages happen, these will damage customer's works but there are still quite many outages occur. Amazon Simple Storage Service (S3) has outage for 2 hour on 15 of February 2008 due to overload of authentication service and another outage for 6 - 8 hours on 20 July 2008 due to single bit error [20]. Window Azure had problem for 22 hours in March 2009 [5]. In 2008, AppEngine's partial outage lasted for 5 hours on 17 June and site of Gmail was unavailable for 1.5 hours in 11 August [20].

Many reasons can cause outages of cloud computing. First reason is natural disasters [5]. In 2009, a lightning striked one Amazon data center and made a 4-hour outage of Amazon's cloud service [5]. Second cause is over-capacity of the cloud [5]. Third reason is a non-technical reason; for example, conflictions of different countries' law can make the outages of cloud computing [20]. Different governments have different regulations and cloud providers will have problems with their services in some countries.

Using many cloud providers is one solution to deal with outages of cloud services [20]. Armbrust et al. [20] indicated that "even if the company has multiple data centers in different geographic regions using different network providers, it may have common software infrastructure and accounting system, or the company may be even go out of business" and these are reasons that cloud services that be provided by one company have more chance to have outages. The unavailability of services can make users and companies to lose a lot of money, so that they should use cloud computing in more prudent ways. They should not "… entrust absolutely mission-critical applications and data to the cloud service providers; and they should use cloud services for non-mission-critical applications and data" [4]. They also should back up their applications and data [4]. Last but not least, they should have a service-level agreement with cloud providers [4, 20]. With this cloud providers will "… offer specialized hardware and software techniques in order to deliver higher reliability…" [20]. When users have this agreement, they will be compensated when outages happen [4].

Data lock-in

An application programming interface (API) is a collection of functions operated by a program and it helps this program to share content and data to other software. The APIs of cloud computing are proprietary and there is no standard for cloud APIs [13, 20]. It is the reason why data and programs cannot be moved easily from one cloud to another. As a result, many companies do not want to use cloud. This challenge makes customers pay more for sole cloud provider and what happen if this exclusive cloud provider goes out of business or have some problems [20]. For example, Linkup was an online storage service which cooperated with Nirvanix, another online storage service, to save customers' information [20]. Nirvanix was sole service provider of Linkup, and when Nirvanix lost data of Linkup's customers, 20,000 users of Linkup found another online storage service and it makes Linkup to go out of business in 8 August, 2008 [20].

One solution for data lock-in was given, cloud providers should use a standard for all APIs and if a cloud provider cannot provide its services, then data and programs from this provider's site can be transferred to another site [20].

Data transfer bottlenecks

Data transfer bottlenecks are another difficulty [20, 23]. Data and applications will be divided and stored at different locations and "… this may complicate data placement and transport" [20]. The cost of moving data is around $100 to $150 per terabyte and it will increase the total costs [20], time consuming is another issue too. One strategy

to solve this difficulty is shipping disks or even ship whole computers [20, 23]. This strategy is not for all circumstances but it will be useful when we need to transfer a larger amount of data [20]. For example, according to an estimation of Armbrust and other authors, transferring ten terabyte from the University of California, Berkeley, to Amazon's headquarters in Seattle with 20 Mbits/sec of bandwidth will cost more than 45 days [20]. Meanwhile if the transfer-disks solution is used, it only cost one day [20].

Reputation fate sharing

There are two aspects in the reputation fate sharing. Firstly, customers who use same cloud will share 'reputation' on this cloud. If one of them does some bad thing on the cloud, he or she will decline the reputation of other people [20]. For example "… blacklisting of EC2 IP addresses by spam prevention services may limit which applications can be effectively hosted [20]. The second aspect is serious: customers who use the same cloud will share 'reputation' and what happen if one company does something illegal [20]? Is there any liable responsibility with other companies which share the same cloud? This problem happen once in March 2009, "… the FBI raided a Dallas data center because a company whose services were hosted there was being investigated for possible criminal activity, but a number of "innocent bystander" companies hosted in the same facility suffered days of unexpected downtime, and some went out of business" [20].

Software license

Customers use many applications with licenses on laptops and personal computers. However many providers have open source applications on their cloud because the license software is not suitable for cloud [20]. It is inconvenient with customers because they are familiar with license software of commercial software company and now they have to use other kinds of software. Commercial software companies can change "… their licensing structure to better fit cloud computing" [20]. To adapt with cloud computing, commercial software companies made their product's version for cloud change to pay-as-you-go strategy for their products. Some big corporations start to apply this approach, Microsoft and Amazon now have version of software for cloud computing with Window Server and Window SQL Server on EC2 and customers have to pay $0.15 per hour [20].

Security in the cloud

The most dangerous barriers of cloud computing is security. There are many affairs of security. The most common security issue of cloud is physical security [2, 24, 25]. Resources are shared between many companies and you do not know where your resources are and you also cannot control resources [2, 24]. When consumers send their data online, it will create chances for other companies, other users take control of their data [2].

According to a research of Cloud Security Alliance (CSA) in 2013 top 9 threats of cloud security are data breaches, data loss, account hijacking, insecure APIs, denial of service, malicious insiders, abuse of cloud services, insufficient due diligence, shared technology issues [26 - 29]. Data breaches happen when malicious people or unauthorized people can access to private, sensitivity or confidential data of cloud's users, data loss happen because of malicious attack, accidental deletion of cloud providers or even catastrophe [26 - 30]. Account hijacking happens when an attacker use stolen credential of customers to access to respective accounts, data or computing services, attack methods are phishing, fraud or use software vulnerabilities [26 - 30]. Application Programming Interfaces are connections between users and cloud providers, API must be designed secure enough otherwise risks will happen [26 - 30]. Denial of service is type of attack when huge amount of requests are sent to cloud server by attackers to consume server's resource such as disk space, bandwidth, and processor power… to prevent cloud server response to legal request from regular customers. Malicious insiders happen when malicious

person (current of previous employee, contractor, third party service providers, business partner…) access to the cloud's data, network or system to do things that can cause negative effect to the confidentiality, integrity, availability of sensitive cloud's data [26, 30]. Abuse of cloud services happen when cloud users use cloud resources to do illegal things to other cloud users or providers [27, 30]. The concern of due diligence is companies or users before moving to cloud lack knowledge of risks associated with cloud and cloud's technology environment [26 - 30]. Cloud computing use sharing technology and multi-tenant architecture and it is hard to build a strong isolated property model, especially with components such as CPU and GPU, this can lead to vulnerabilities of shared technology [26 - 30]. When resource such as CPU are shared between many cloud users then in some cases, sensitive data of a user can be exploited by other users who use the same cloud [31]. Kazim and Zhu [27] group these security issues to three groups, data security group contains data breaches and data loss, network security group contains account hijacking, denial of service and cloud environment security contains insecure APIs, malicious insiders, abuse of cloud services, insufficient due diligence, shared technology issues. Report of CSA in 2016 adds three more security concerns which are insufficient identify, credential and access management, system vulnerabilities and advanced persistent threat [30].

There are also more security problems with the cloud. Some authors mentioned about security issues that related to service models (IaaS, PaaS, and SaaS) of cloud [32 - 34]. The issues of IaaS are mostly related to virtual technology such as virtual machine image sharing, virtual machine isolation, virtual machine escape, virtual machine migration, virtual machine rollback, virtual machine sprawl, hypervisor security …, the security problems of PaaS are SOA related security issues, the security problems of SaaS are data security, application security [32 - 34]. From all these security issues, virtualization security is one of the most serious one because virtualization technology is critical technology of the cloud [26, 32, 35, 36].

CONCLUSIONS

Cloud computing is a very attractive technology for developing, because it has many advantages. Cloud computing can transfer from capital expense to operational expense so that cloud providers will save costs, this architecture also can save costs for customers because they only has to pay for what they use and this model is called pay-as-you-go. Resources of cloud computing are very elastic, resources can be provided to users when they demand and can be disposed when they do not demand. Resource pooling is another advantage of cloud computing, all resources are shared between users by a homogeneous infrastructure. Through cloud computing, human interaction between customers and cloud providers is not necessary, users can contact with cloud providers by web portal or management interface, this new infrastructure is self-service information technology infrastructure. With the assist of cloud computing, service can be measured correctly although many customers use same service.

However, there are still some challenges with cloud computing. Availability of service is the first issues, many big providers of cloud computing like Amazon, Windows and Google now struggle with this problem, because all of them are experienced with out of service time of their 'cloud' and if outages will make huge problems for cloud's customers. Data lock-in is another issue; customers will have many difficulties to transfer data, applications from one cloud to other clouds of other cloud providers. In cloud computing, data will be stored at different locations and it will cause many problems related to storing and transferring data, this challenge is called data transfer bottlenecks. All customers or organizations which share same cloud will have same reputation and all customers, organizations will have problems if one of them do illegal things, this

affair prevent development of cloud computing, many corporations dare not using cloud computing. Software companies which made commercial software also need to change their licensing to adapt with the cloud. Last but not least, security is a big problem with cloud computing.

REFERENCES

1. M.D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, A. Vakali, A. 2009, Cloud computing: distributed internet computing for IT and scientific research, Internet Computing, IEEE, 13, (5), 2009, 10-13.
2. J.W. Rittinghouse, J.F. Ransome, Cloud computing: implementation, management, and security, CRC Press, Boca Raton, 2010.
3. Z. Shuai, Z. Shufen, C. Xuebin, H. Xiuzhen, Cloud computing research and development trend, Future Networks, 2010, ICFN '10 Second International Conference, Sanya, Hainan, pp. 93-97.
4. W. Kim, S.D. Kim, E. Lee, S. Lee, Adoption issues for cloud computing, MoMM '09: Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia, ACM, Kuala Lumpur, Malaysia, 2009, pp. 2-5.
5. S. Paquette, P.T. Jaeger, S.C. Wilson, 2010, Identifying the security risks associated with governmental use of cloud computing, Government Information Quarterly, 27, (3), 2010, 245-253.
6. D.B. Hoang, T.D. Dang, Health Data in Cloud Environments, 19th Pacific Asia Conference on Information Systems (PACIS 2015).
7. S.J. Miah, J. Hasan, J.G. Gammack, On-Cloud Healthcare Clinic: An e-health consultancy approach for remote communities in a developing country, Telematics and Informatics, 34, (1), 2017, 311-322.
8. N. Sultan, Making use of cloud computing for healthcare provision: Opportunities and challenges, International Journal of Information Management, 34, (2), 2014, 177-184.
9. S. Deng, L. Huang, J. Taheri, A.Y. Zomaya, Computation offloading for service workflow in mobile cloud computing', IEEE Transactions on Parallel and Distributed Systems, 26, (12), 2015, 3317-3329.
10. M. Othman, S.A. Madani, S.U. Khan, A survey of mobile cloud computing application models, IEEE Communications Surveys & Tutorials, 16, (1), 2014, 393-413.
11. Y. Wang, R. Chen, D. Wang, A survey of mobile cloud computing applications: perspectives and challenges, Wireless Personal Communications, 80, (4), 2015, 1607-1623.
12. A. Botta, W. De Donato, V. Persico, A. Pescapé, Integration of cloud computing and internet of things: a survey, Future Generation Computer Systems, 56, 2016, 684-700.
13. D.S. Linthicum, Cloud computing and SOA convergence in your enterprise: a step-by-step guide, Addison-Wesley Professional, 2009.
14. M. Creeger, 2009, Cloud computing: An overview, ACM Queue, 7, (5), 2009, 1-5.
15. H.G. Miller, J. Veiga, Cloud computing: will commodity services benefit users long term?, IT Professional, 11, (6), 2009, 57-59.
16. T. Dillon, W. Chen, E. Chang, Cloud computing: issues and challenges, Advanced Information Networking and Applications (AINA), 24th IEEE International Conference, Perth, WA, 2010, 27-33.
17. T. Mather, S. Kumaraswamy, S. Latif, Cloud security and privacy, 1st ed., O'Reilly, Beijing, 2009.
18. Agence France-Presse 2010, Fujitsu, Microsoft in cloud computing tie up, The Morning Sydney Herald , viewed 6 January 2017, <http://news.smh.com.au/breaking-news-technology/fujitsu-microsoft-in-cloud-computing-tie-up-20100713-108zd.html>.
19. J. Chong, Optus offers cloud computing, The Morning Sydney Herald, viewed 6 January 2017, <http://news.smh.com.au/breaking-news-business/optus-offers-cloud-computing-20100914-15aoz.html>.
20. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, A view of cloud computing, Communications of the ACM, 53, (4), 2010, 50-58.

21. D. Durkee, Why cloud computing will never be free, Communications of the ACM, 53, (5), 2010, 62-69.
22. B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud-computing vulnerabilities', Security & Privacy, IEEE, PP, (99), 2010, 1-14.
23. Y. Han, On the clouds: a new way of computing, Information Technology & Libraries, 29, (2), 2010, 87-92.
24. K. Popovic, Z. Hocenski, Cloud computing security issues and challenges, MIPRO, 2010, Proceedings of the 33rd International Convention, Opatija, Croatia, pp. 344-349 .
25. G. Zhao, C. Rong, M.G. Jaatun, F.E. Sandnes, Deployment models: towards eliminating security concerns from cloud computing, High Performance Computing and Simulation (HPCS), 2010 International Conference, Caen, France, 2010, pp. 189-95.
26. T. Islam, D. Manivannan, S. Zeadally, A classification and characterization of security threats in cloud computing, Int.J.Next-Gener. Comput, 7, (1), 2016.
27. M. Kazim, S.Y. Zhu, A survey on top security threats in cloud computing, International Journal of Advanced Computer Science and Applications (IJACSA), 2015.
28. C. Prakash, S. Dasgupta, Cloud computing security analysis: Challenges and possible solutions, Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on IEEE, 2016, 54-57.
29. A. Sharif, S. Cooney, S. Gong, D. Vitek, Current security threats and prevention measures relating to cloud services, Hadoop concurrent processing, and big data, Big Data (Big Data), International Conference on IEEE, 2015, pp. 1865-1870.
30. Cloud Security Alliance, The Treacherous Twelve' Cloud Computing Top Threats 2016, viewed 2 January 2017, https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/>.
31. M.S. Inci, B. Gülmezoglu, T. Eisenbarth, B. Sunar, Seriously, get off my cloud! Cross-VM RSA Key Recovery in a Public Cloud., IACR Cryptology, 2015.
32. M. Almorsy, J. Grundy, I. Müller, An analysis of the cloud computing security problem', APSEC 2010 Proceeding-Cloud Workshop, 2010.
33. K. Hashizume, D.G. Rosado, E. Fernández-Medina, E.B. Fernandez, An analysis of security issues for cloud computing, Journal of Internet Services and Applications, 4, (1), 2013, 5.
34. D. Puthal, B. Sahoo, S. Mishra, S. Swain, Cloud computing features, issues, and challenges: a big picture, Computational Intelligence and Networks (CINE), International Conference on IEEE, 2015, pp. 116-123.
35. M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: Opportunities and challenges, Information Sciences, 305, 2015, 357-383.
36. S. Farahmandian, D.B. Hoang, Security for software-defined (Cloud, SDN and NFV) infrastructures- issues and challenges, Eight International Conference on Network and Communications Security, 2016.