IJCCN | INTERNATIONAL JOURNAL OF COMPUTING & COMMUNICATION NETWORKS

Vol. 2, Issue 1, February 2020

Security Threats in Cloud Computing: Trend and Challenges

Kaneez-e-Rubab[1], Talha Azhar[1], Muhammad Anwar[2], Saqib Majeed[3]

[1] Department of Computer Science, Bahria University, Islamabad, Pakistan

[2]University of Education, Lahore, Pakistan

[3]University Institute of Information Technology, PMAS-AAUR, Rawalpindi, Pakistan

* Corresponding Author: Kaneez-e-Rubab

Received 20 December 2019; Revised 15 January 2020; Accepted 25 January 2020; Published 24 February 2020

Abstract: Recently due to the increasing popularity of cloud computing, the people are attracting their services and offers without knowing the security threats. Users think that that cloud is more secure as compared to any other services. This fact leads to serious problems for users. This is why the security of the cloud has become a major issue. In this paper, we investigate the recent and most common threats of cloud computing. After a detailed investigation, we discuss the seven major threats related to cloud computing. These risks are related to cloud computing and are the main guidance for risk analysis for organizations or customers to switch their services on the cloud computing platform. The organization or customers must know about these threats before adapting any cloud service or interface. This paper will guide the new researchers in the field of cloud computing and its security services to design more secure and reliable solutions in the future.

Keywords: *Cloud, Challenges, Security, Threats, Attacks, Layers, Models*

1. Introduction

Cloud computing is based on hardware and software components to deliver different processing, storage, and analysis services over the network. Through cloud computing, users can easily access their files and also use applications from any device by using the Internet such as Gmail, Dropbox, and Skype applications. Cloud is a big pool of accessible and usable virtualization resources. Nowadays, due to the low prices of cloud computing platforms,' it became the most relevant and famous thing in IT businesses. So, all the major companies like Microsoft, Amazon, and Google are using cloud computing. The system of cloud computing consists of two ends: the front end and the back end. The front end is a user end or user interface where the user is accessing services from the cloud through his devices. The back end is a cloud of the system where all the services and information are stored [1, 2]. According to the research in [3], nowadays cloud computing lies in the top ten technologies. Cloud computing is like a computer prototype and it is a distributed architecture which is distributing all the resources, services, and data over the network insecure, efficient, and timeless manner. It is fulfilling all the functional and non-functional requirements like availability, security, agility, scalability, and reliability. It is a combination of many technologies like Service Oriented Architecture, Business Models, and Virtualization. The cloud computing services have proved better services as compared to traditional old services.

Cloud computing is reaching towards the points where computing things have great potential and promising functions which we cannot yet imagine. It is a new concept that has the goal to make computational resources available as services on demand in limited time and minimum cost. It is based on three business models: SaaS (Software-as-a-Service), IaaS (Infrastructure-as-a-Service), and PaaS (Platform-as-a-Service) [4, 5]. The key functions of business models are as follows:

- **SaaS** allows the customers to run their applications with the help of visualization hardware on the cloud provider resources like Salesforce Customers Relationship Management (CRM).
- **IaaS** provides a container environment for customers to deploy their custom applications with their dependencies like Google App Engine.
- **PaaS** provides hardware platforms in the form of services such as database services, network services like Amazon Elastic Compute Cloud (EC2).

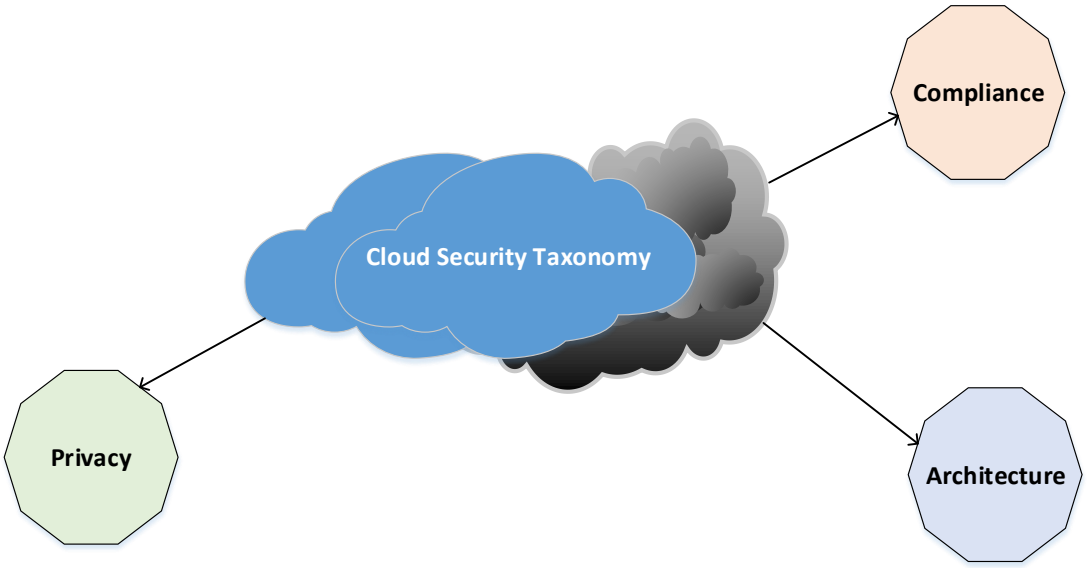

Figure 1: Cloud Security Taxonomy [6]

Cloud computing consists of five essential characteristics which are On-demand Self-service, Broad network access, Resource pooling, Rapid elasticity, and Measured services. It also consists of three deployment models Public, private, and Hybrid [5]. Figure 2 shows the three deployment models of cloud computing.

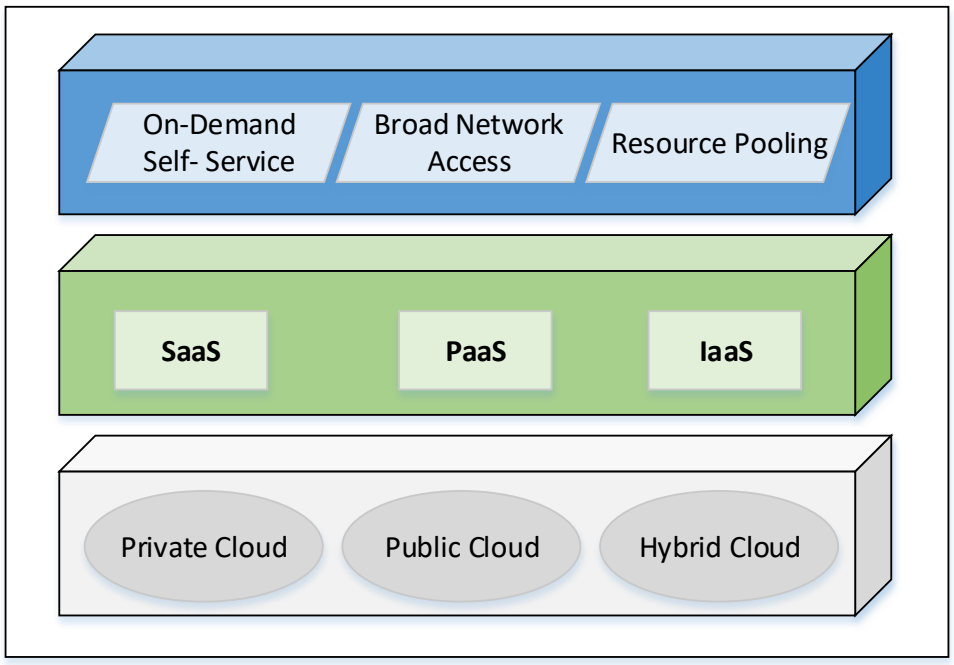

Figure 2: Cloud Deployment Models

Private cloud is based on a private setup like an organization's internal data center, in this, the cloud vendors provide services to the organization, and the resources and applications are managed by the organization itself. Only some people can access the information. On the other hand, public clouds can be accessed by many people like through the internet, billing, etc. These clouds are less secure than the other models. A hybrid cloud is basically a mixture of public and private clouds. It is a more secure model than others. It's a combination of virtual and physical assets [7]. This paper main objective is to investigating the recent security threats in cloud computing and possible solutions to protect the user data and make cloud services more reliable and beneficial. The other objectives of this paper are as follows:

- Discuss the cloud computing architecture to understand the services and layers of cloud computing
- Discuss the recent threats faced by cloud computing services
- Discuss the abuse and nefarious use of cloud computing

The remaining paper is organized as follows. Section 1 explains what is cloud computing and also its business models. Section 2 describes the main architecture of cloud computing and the diagram 1 in this section describes the main four layers and the key functions of the layer. In section 3 we generally describe the main seven problems related to security of cloud computing. In sections 4, 5, 6, 7, 8, 9, and 10 we discuss the literature of each security threat. Section 11 concludes this paper.

2. Cloud Computing Architecture

The cloud computing architecture is divided into four layers the Resources and Network layer, Services layer, Access layer and User layer. Here are the key functions of all the four layers [8]:

- The Resources and Network layer manages all the resources like physical and virtual
- The Services layer deal with all the services like SaaS, PaaS, and IaaS
- The Access layer deal with the access functions and the inter point functions
- The User layer deal with the user functions, partner functions and the administration functions

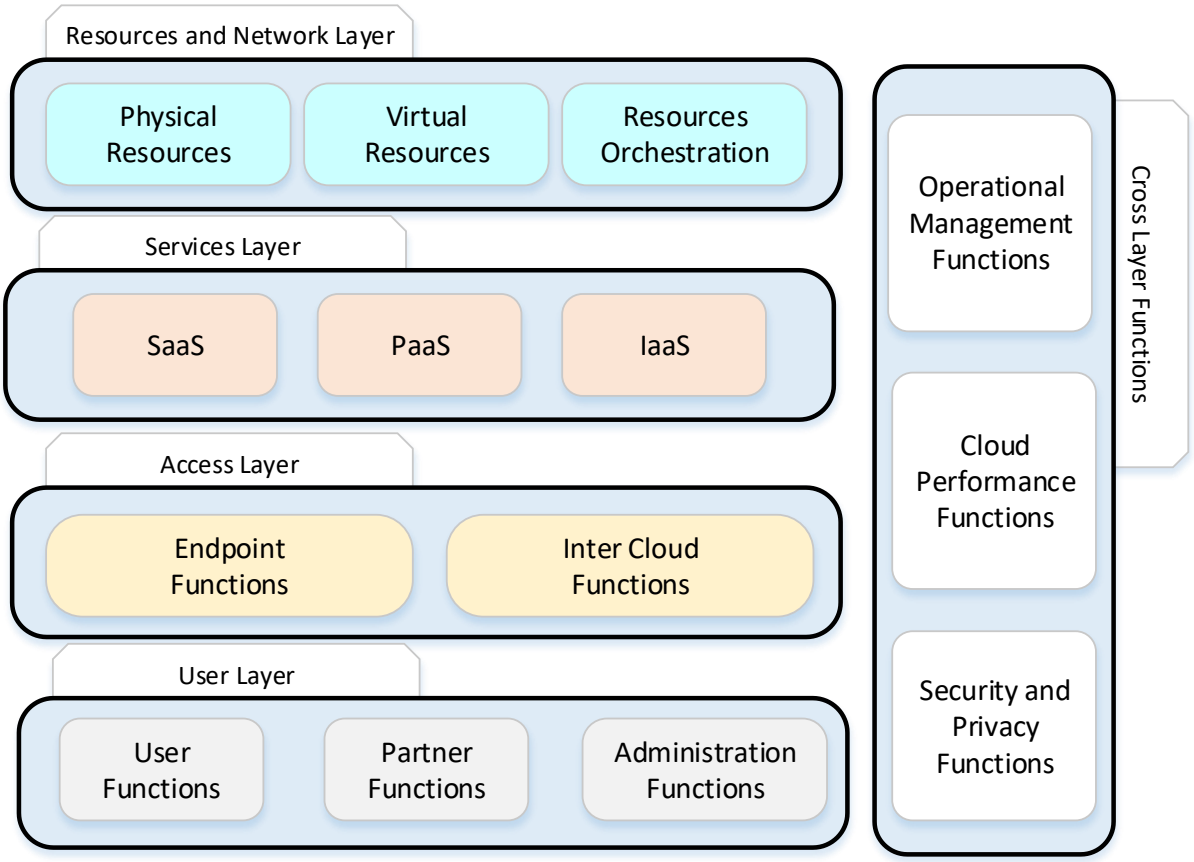

Figure 3: Four layers and Their Key Functions

3. Threats to Cloud Computing

Security is one of the main concerns of cloud computing this is why the researches are more concerned about the security of clouds. In this section, we review the main security threats related to cloud computing. These security threats can be classified into seven main categories which are abuse and nefarious use of cloud computing, insecure application programming interfaces, malicious insiders, shared technology vulnerabilities, data loss, account service, and traffic hijacking and unknown risk profiles [9]. These risks are related to cloud computing. These are the main guidance risks and organizations must know about these risks before adopting any cloud interface or services. In this section, we discuss these seven threats.

Cloud abuse is one of the top threats of cloud computing. It is related to that situation when hackers use social media to abuse cloud environments or a false registration process. Anyone can register with a valid credit card in a limited trial period. The hackers can hack the real accounts and all the information related to their credit cards and accounts. SaaS and PaaS providers are facing this type of threat [10]. The second threat is related to the insecure interfaces and Application Programming Interfaces (APIs) where the cloud providers expose numerous interfaces especially for the customers so they can interact and get cloud services very easily. But this comes in security threat because the availability and security of these cloud services depend upon the security of those expose APIs and interfaces. All three models IaaS, SaaS, and PaaS are related to this security issue. The third threat is malicious insiders which is the more well-known and famous threat among organizations. This threat is related to the information technology and the employees of cloud providers mean the inside employees are a big threat to services and privacy [11]. They have access and they can use this access in the wrong way. IaaS, SasS, and PaaS all three service models are related to this threat. The next threat is about issues of sharing of technology. Like the cloud providers deliver their services by sharing infrastructure. This sharing technology became the issue of security because the customers are sharing resources, platforms. Just IaaS service model is related to this threat because it is providing share infrastructure, and platforms.

The fifth threat is data loss which is the most common threat to everything, especially for a cloud. Like data is the loss of leak because it is stored on the unreliable media or there is no record of the larger context data. It is becoming lost or there's no backup of data and it got loss. Encoding decoding is another reason for data loss. Like data is lost because the encoded files get affected by a virus or the encoding wasn't done well. All the three service models related to this threat. The sixth threat related to cloud security is the account or service hijacking. It is related to the hacking of users accounts or services by using password reuse or any other technique for hijacking. If the attackers gain access to your account, eyes drop on all your activities and redirect your clients to someone else. IaaS, PaaS, and SasS all the three service models come under this threat. Last but not the least threat is profiles of unknown persons which is a big risk to cloud providers as well as the customers. This is also a common threat among organizations. Like the lack of information about those profiles and don't know their purpose [9].

3.1 Abuse and Nefarious Use of Cloud Computing

According to authors in [12], Abuse and Nefarious" is the top security threat in cloud computing. In this, any person with a valid credit card can easily register on the cloud. There is no restriction for the registration process. So, the fraud persons can easily register themselves pretend to be customers, and then start their fraud work. Because of this flaw, full registration process, the attackers attack the services models and start target cloud providers. Some cloud providers offer trial versions [12]. That is a great opportunity for the criminals to register themselves with the free version. There are many data centers of cloud computing and each data center is located at a different location and involves many customers where a huge amount of data exists. This will make fraud detection more difficult for cloud providers. Figure 4 shows the different security requirements components which makes a more difficult task to handle security.

According to authors in [13], there are several major attacks connected to "Abuse and Nefarious Use of Cloud computing". There is an attack which is called "Host hopping". In this attack, the hackers can easily gain illegal access to customer's data by attacking resource sharing characteristics of clouds e.g. storage, memory, etc. there's a second attack which is known as "Malicious insider and use of privileges". In this attack, the insiders can hack or share the data which we will discuss in the next heading. There is another attack in which the service engines compromised. Cloud providers control this engine but sometimes it can be rented by any customer who wants to adopt the IaaS model. Hackers can easily abuse this engine by renting any Virtual Machines (VM) and hack the service engine from the inside and use it for their bad purpose like accessing confidential data.

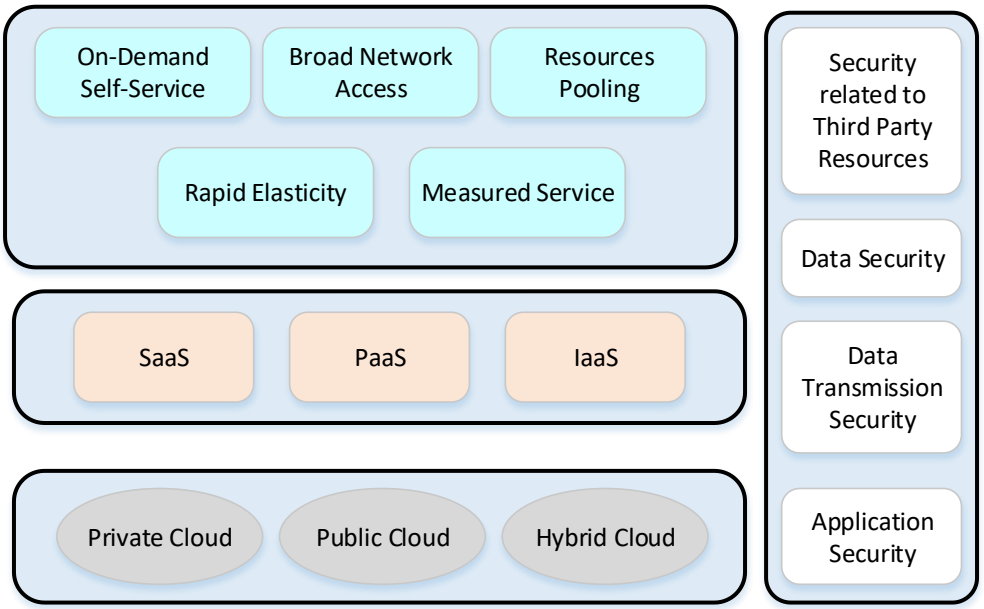

Figure 4: Cloud Environment Complexity [13]

3.2. Malicious Insiders

Everyone is familiar with "Malicious Insiders". According to authors [14], they are the current or former employees or any other person who has a direct or indirect link to the services, data. They misuse the data and affect the availability, confidentiality of the data of customers, and the cloud itself. They can easily host sensitive information to multiple clients or leak or sell the information to other competitive business parties. These hackers can easily set up fake accounts because they knew about all the inside things so they can sell or leak confidential information of customers [13].

3.3. Insecure APIs

Cloud providers expose different software or programming interfaces to their customers so they can easily use their services. The all nonfunctional requirements depend upon the security of these interfaces [9]. Each cloud has its APIs which need to be installed before using that cloud services. these APIs get affected by HTML, XML, and Denial of service attacks (DDOS) [15]. But DDOS attacks are more dangerous than all other attacks because in this all resources are placed at a single place so distributors can easily attack all the resources at a single time. So, these insecure APIs make the cloud vulnerable to different types of security attacks [16].

3.4. Shared Technology Vulnerabilities

The cloud environment is based on sharing infrastructure [9]. Many users are sharing the same technology at same time. So basically, there is a hypervisor which acts as a mediator between guest Many users are sharing the same technology at the same time. So basically, there is a hypervisor that acts as a mediator between the guest Operating System and the physical interfaces. All the users are on the top layer of that hypervisor. So if the hypervisor security became compromised the entire cloud will get affected [16]. Security and availability of the cloud depend on the security of these APIs. For the security of cloud services, these vulnerabilities should be checked before delivering the cloud services to customers [17].

3.5. Data Loss

Here comes the data loss issue in cloud computing. Data loss can be in many forms such as deletion of data, didn't make the backup of data or data moving in the data centers and lost in the way, etc. it will be difficult to retrieve the data or get track of the data [18]. There is another challenge which is basically a major challenge related to data. All the data placed on the data centers and sometimes the hacker's direct attack the datacenters to destroy the whole data center or to shut down the servers. Hackers use different approaches to attack the data centers like put a virus in one file which corrupts the whole system or leaks the data so the customer's confidentiality and clouds image became compromised and the competitors can easily get the benefits from this bad situation [19].

3.6. Account or Service Hijacking

Accounts or service hacking is a common threat in any kind of model. There are different methods to hack the accounts like cracking passwords, malicious insiders leak or sell the confidential information to hackers or competitors, etc., Through this attacker can easily get access to the critical areas and the confidentiality, reputation of clients and cloud providers became compromised [20]. There is another way of hijacking account by using native APIs for login and anyone can easily register himself and hack the account [21].

3.7. Unknown Risk Profile

Before adopting any cloud interface, the user must gain some knowledge about that cloud. After adopting the cloud services, the user must know where their data and related logs are stored because there is a big challenge of unknown risk profiles [22]. According to authors [23], Security must not be lost between the benefits of hardware and software. Because if that happens, the risks of unknown profiles will come because customers don't know about the code updates, how their data and logs are stored and who has access to them, etc. [24].

Conclusion

Nowadays Cloud computing is the most thing in information technology. Everything is on the cloud and people can easily access it from anywhere through the internet. So, all the big organizations are using these services. But it has many security issues. In this paper first, we discussed in detail what is cloud computing. Then we discussed cloud computing architecture in detail. Its three service models SaaS, PaaS, and IaaS. Then cloud computing deployment models Public, Private and Hybrid and then five major and essential characteristics of cloud computing models e.g. on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. And at last, we surveyed the seven major threats related to cloud computing whichever organization should know before going on any cloud. We present a survey that covered these seven major threats related to cloud computing.

References

[1] V. Kumar, "Survey Paper on Cloud Computing," *International Journal of Engineering Advanced Technology*, vol. 2, no. 6, pp. 160-162, 2013.

[2] K. N. Qureshi, F. Bashir, and S. Iqbal, "Cloud computing model for vehicular ad hoc networks," in *2018 IEEE 7th international Conference on Cloud Networking (CloudNet)*, 2018, pp. 1-3: IEEE.

[3] M. B. A. Malar and J. Prabhu, "AN ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING."

[4] A. Gholami and E. Laure, "Security and privacy of sensitive data in cloud computing: a survey of recent developments," *J arXiv preprint arXiv:.01498*, 2016.

[5] K. N. Qureshi, F. Bashir, and A. H. Abdullah, "Provision of security in vehicular ad hoc networks through an intelligent secure routing scheme," in *2017 international conference on frontiers of information technology (FIT)*, 2017, pp. 200-205: IEEE.

[6] N. Gonzalez, C. Miers, F. Redigolo, M. Simplicio, T. Carvalho, M. Näslund, and M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing," *Journal of Cloud Computing: Advances, Systems Applications*, vol. 1, no. 1, p. 11, 2012.

[7] S. Kuyoro, F. Ibikunle, and O. Awodele, "Cloud computing security issues and challenges," *International Journal of Computer Networks*, vol. 3, no. 5, pp. 247-255, 2011.

[8] K. Lee, "Security threats in cloud computing environments," *International journal of security its applications*, vol. 6, no. 4, pp. 25-32, 2012.

[9] C. S. Alliance, "Top threats to cloud computing v1. 0," *White Paper*, vol. 23, 2010.

[10] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *JOURNAL OF AMBIENT INTELLIGENCE AND HUMANIZED COMPUTING*, 2020.

[11] M. S. Aliero, K. N. Qureshi, M. F. Pasha, I. Ghani, and R. A. Yauri, "Systematic Review Analysis on SQLIA Detection and Prevention Approaches," *Wireless Personal Communications*, pp. 1-37, 2020.

[12] M. Blumenthal, "Is security lost in the clouds?," *Communications Strategies*, no. 81, pp. 69-86, 2011.

[13] M. Omar, "Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing," in *Handbook of Research on Security Considerations in Cloud Computing*: IGI Global, 2015, pp. 30-38.

[14] A. J. Duncan, S. Creese, and M. Goldsmith, "Insider attacks in cloud computing," in *2012 IEEE 11th international conference on trust, security and privacy in computing and communications*, 2012, pp. 857-862: IEEE.

[15] T. Karnwal, T. Sivakumar, and G. Aghila, "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack," in *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, 2012, pp. 1-5: IEEE.

[16] H. Jelodar and J. Aramideh, "Common techniques and tools for the analysis of open source software in order to detect code clones: A study," *International Journal of Electronics Information Engineering,* vol. 1, no. 2, pp. 64-69, 2014.

[17] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *The journal of supercomputing,* vol. 63, no. 2, pp. 561-592, 2013.

[18] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," *Procedia Engineering,* vol. 15, pp. 2852-2856, 2011.

[19] L. Malhotra, D. Agarwal, and A. Jaiswal, "Virtualization in cloud computing," *J. Inform. Tech. Softw. Eng,* vol. 4, no. 2, pp. 1-3, 2014.

[20] V. Pandey and M. Dubey, "IDS CRITERIA FOR ENHANCED SECURITY OVER CLOUD," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 7, 2017.

[21] Y. An, Z. Zaaba, and N. Samsudin, "Reviews on security issues and challenges in cloud computing," in *IOP Conference Series: Materials Science and Engineering*, 2016, vol. 160, no. 1, p. 012106: IOP Publishing.

[22] M. A. Bamiah and S. N. Brohi, "Seven deadly threats and vulnerabilities in cloud computing," *International Journal of Advanced engineering sciences technologies,* vol. 9, no. 1, pp. 87-90, 2011.

[23] S. Walia, "Security and Privacy issues in Cloud Computing."

[24] M. Theoharidou, N. Tsalis, and D. Gritzalis, "In cloud we trust: Risk-Assessment-as-a-Service," in *IFIP International Conference on Trust Management*, 2013, pp. 100-110: Springer.