Cloud Computing Security: Issues and Developments

Isaac Odun-Ayo, *Member, IAENG*, Olasupo Ajayi and Sanjay Misra

Abstract- **Cloud computing is a technology paradigm that is offering useful services to consumers. Cloud service providers utilize huge computing resources spread over geographical distances to provide services to customers. The computing resources deployed over the Internet comprises hardware and software used in virtualization, storage and compute purposes. This has obvious security implications as data is transmitted and stored in different locations over the Internet. Such data is not within the control of the owner. Beyond data, there are other security issues in cloud computing relating to virtualization and applications. Security has severe impact on the decision as to whether an organisation will adopt the cloud or not. Hence, the discussion on security is dynamic and solutions are evolving daily. This paper examines present trends in the area of cloud security and provides a guide for future research. In the present work, the objective is to answer the following question: what is the current trend and development in cloud security? Papers published in journals, conferences, white papers and those published in reputable magazines were analysed. The expected result at the end of this review is the identification of trends in cloud security. This will be of benefit to prospective cloud users and even cloud providers.**

Index Terms **- Cloud Computing, security, infrastructure, services**

I. Introduction

"CLOUD computing is a model for enabling universal, on-demand and convenient network access to a shared pool of configurable computing resources (e.g., servers, applications, storage, networks and services) that can be quickly provisioned and released with little to no management effort or service provider interaction" [1]. Cloud computing is a networked system of computer resources available on demand with minimum interaction by users [2]. Cloud computing aims to provide computing power, storage and software including infrastructure on demand [3]. Cloud computing leverages on existing technologies including the Internet to provide services to customers. The cloud has four deployment models namely: private, public, community and hybrid clouds. The public cloud infrastructure is made available to enterprises requiring services and it is owned by a CSP [3]. The private cloud is owned by an enterprise or organisation with control over the infrastructure because users are in-house staff [4]. The community cloud infrastructure is owned and controlled by multiple organizations with shared common interest [5]. The hybrid cloud deployment model is an aggregation of the private, public or community cloud. This allows for the leveraging of the benefits available in these cloud types.

Cloud computing has three service models, the Software-as-a-Service (SaaS), Platform-as–a–Service (PaaS) and Infrastructure–as–a–Services (IaaS). The SaaS model entails a CSP making an application available to the consumer and such an application runs on the cloud infrastructure [3]. PaaS refers to services where a consumer can create and deploy an application on a CSP's infrastructure. IaaS provides physical machines, virtual machines, storage and compute resources to consumers [6]. Cloud computing security involves all issues that make the cloud secure. Cloud security includes the design of architecture, attack surfaces, protection from various forms of attack and access controls [7]. Security concern is not peculiar to the cloud alone, but certain things make cloud security unique. Resources are shared on the cloud and a tenant may be malicious. Cloud based data is accessible to most cloud users, but the protocols and application programming interfaces used makes the cloud insecure. [7] Data in the cloud can have its integrity compromised or lost. An enterprise or individuals data in the cloud is available to the CSP and others users [7].

The major concerns in terms of data on the cloud are to ensure authorization, authentication, confidentiality, availability and integrity. In view of the fact that several users access common resources, authorization is essential to secure data. It is also important to ensure adequate authentication and identification of cloud users to prevent unauthorized access [8]. Data integrity ensures that data provided by user is not modified in any form. Data confidentially is of prime importance on the cloud because no user expects leakage of stored data. However, this is difficult to maintain because several users including the CSP and their staff have access to shared resources. Availability of data ensures that data is available to the user, anywhere at any time [8].

Availability of data is an aspect of the service level agreement between the CSP and customers that is given priority attention. The importance of security in cloud computing cannot be overemphasized. In the 2016 IDG survey, security was among the top three concerns for utilizing public, private and hybrid clouds with a result of 41%, 21% and 24% respectively [9]. The focus of this paper, therefore,

Manuscript received December 05, 2017; revised January 05, 2018. This work was supported in part by the Covenant University through the Centre for Research, Innovation and Discovery (CUCRID).

I. Odun-Ayo is with the Department of Computer and Information Sciences, Covenant University, Ota, Nigeria. (+2348028829456; Isaac.odun-ayo@covenantuniversity.edu.ng)

O. Ajayi is with University of Lagos, Lagos, Nigeria. (Olasupo.ajayi@unilag.edu.ng)

S. Misra is with the Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria (sanjay.misra@covenantuniversity.edu.ng).

is to examine cloud computing security issues. As cloud computing is evolving, so also are the security concerns. Various kinds of security threat available in cloud computing will be discussed and possible solutions proffered. Current issue in cloud computing from the perspectives of industry will be highlighted. This becomes necessary because of little or no synergy between research and current industry trends. The paper is structured as follows, Section 2 presents related work, Section 3 examines cloud concerns and possible solutions, Section 4 highlights current industry concerns in cloud security, Section 6 involves analysis and discussion, and Section 7 is the conclusion, with suggestions for future research.

II. Related Works

Data Security Challenges and Its Solutions in Cloud Computing in [10] discussed various data security challenges and proposed some solutions. Some aspects of data security ranging from use of application, storage and network was discussed. Cloud Computing Challenges and Solutions in [7] examined some cloud security attacks from the perspective of the cloud service provider and at the network level. It presumed that cloud attacks could come from different sources and suggested some possible solution. Customer Security in Cloud Computing in [3] focuses on data confidentiality, integrity and availability. The paper considers that the level of cloud usage will be directly proportional to the level of cloud security. A Survey on Cloud Computing Security: Issues, Solution and Threats in [11] conducted an overview of cloud security concerns such as sharing and virtualisation of resources. Thereafter, solutions were proffered with a view to enhancing security on the cloud. A Survey of Security Issues for Cloud Computing in [6] took a detailed look at various threats to cloud computing security and conducted a comprehensive analysis. Furthermore, several aspects of cloud security were discussed and some solutions proffered. Your Top 5 Cloud Data Protection Challenges Solved in [12] is an industry perspective to the issues of security in the cloud. It presented five challenges that concerns cloud user in term of data security and proffered possible solutions. State-of-the-art Survey on Cloud Computing Security

Challenges, Approaches and Solutions in [13] examined security issues in the cloud. Thereafter, a case study of Amazon Web Services was used to discuss security measures in place to mitigate security concerns. Data Security Challenges in Cloud Computing and Its Solutions in [14] examined various levels of data insecurity. Reviews on Security Issues and Challenges in Cloud Computing in [15] examined security, privacy, application and threat issues. The security issues were further discussed and a wide range of security solutions were suggested. Security in Cloud Computing: Opportunities and Challenges in [16] proposed a cloud computing architectural framework. Security challenges at various abstractions of cloud computing were examined. Thereafter, the security solutions in literature were discussed. Finally, security issues in mobile cloud computing were also examined.

Towards Multi-Stage Intrusion Detection using IP Flow Records in [4] proposed a model for intrusion detection. The focus was on malicious flow and the proposed model was also implemented. Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework in [2] conducted a security survey through interviews, literature and discussion with cloud developers. It examined security in terms of web application, data hosting and virtualization. Cloud Computing Security: A Systematic Literature Review in [8] presented a survey of security risk on the cloud and the security solutions proposed in those surveys. It proposes the importance of security discussions in the areas of software and hardware integrity, service models and deployment types.

Defining Security for Today's Cloud Environments in [5] provides an industry perspective to cloud security. The focus is on the current security measures for the cloud deployment types. Data Classification for Achieving Security in Cloud Computing in [17] proposes parameters for classifying data for security purposes on the cloud. The aim is to provide security for data in storage in the cloud based on the level of classification. Data and Infrastructure Security Auditing in Cloud Computing Environment in [18] proposes cloud security auditing from three perspectives. The aim was to examine infrastructure and data security auditing. Cloud Computing Security:

The Scientific Challenge, and a Survey of Solutions in [19] proposes an encryption standard for security on the cloud. It examines four approaches with the aim of ensuring that the cloud provider does not see plain text. Cloud Computing Adoption Framework: A Security Framework for Business Clouds in [20] proposes a security framework for the cloud based on firewall, identity management and encryption. The framework was implemented in various aspects of security and it shows a high level of effectiveness. Cloud Computing Security Issues and Challenges: A Survey in [21] presented a survey of security issues in terms of cloud delivery and deployment modes. It also examined security in other vital areas of cloud computing.

III. SECURITY ISSUES IN CLOUD COMPUTING

Security concerns cuts across the entire spectrum of cloud computing. Security affects the communication, architectural and contractual levels. Communication on the cloud is done through the Internet using standard transmission protocols for transfer of data between the cloud customer and cloud infrastructure [12]. The security issues over the Internet include denial of service, eavesdropping, IP–spoofing based flooding and masquerading, while solution to these include secure socket layer, cryptography, intrusion prevention systems and digital certificates [12]. Internal communication security issues affect shared communication infrastructure, virtual network and security configurations. Cloud users are usually granted access for managing virtual machines and a malicious user could launch attack such as sniffing and spoofing. The virtualized network is used for communication among virtual machines; and because it is shared, it could allow for attacks such as denial of service, spoofing and sniffing of the virtual network, leading to data insecurity [12]. Migration of VMs, data or weakness in session and protocol configuration can also affect user data on the cloud.

A. Architectural challenges

1) Virtualization issue

Virtualization allows several cloud users to share the resources on a physical machine. The Virtualisation Machine (VM) process is managed by a hypervisor. Virtualisation presents several security concerns. VM sharing grants user's ability to upload or download images from the repository [12]. Malware could be embedded into the image to be uploaded leading to data breaches. Thus giving malicious users the ability to determine the security state of the platform. There could also be VM isolation among users, access to the same physical resources on the cloud could lead to cross–VM attacks, hence isolation must include computational resources too [12]. The virtual machine manager (VMM) or hypervisor is used to manage the VMs and it also controls access to resources. A VMM escape allows a malicious user to evade the VMM control, leading to illegal access to storage and compute resources.VM migration allows the transfer of a VM to another physical machine for the purpose of load balancing or maintenance [12]. If this is not done properly, a malicious attacker can relocate a VM to another server leading to data leakage. VM rollback restores a virtual machine to a previous state, leading to the enabling of stored security credentials which can jeopardize data security. The hypervisor or VMM is the heart of the virtualization process, if a malicious user takes control of the VMM or if there are bugs in the VMM, this could lead to exposure of user data on the cloud.

2) Data storage issue

Lack of user control over his/her data could lead to the compromise of data integrity and privacy. The CSP is charged with managing servers and data for users [12]. The multi-tenancy nature of the cloud and the presence of a malicious user can lead to unauthorized access to all user data. Data recovery vulnerability entails assigning data recovered from one user to another user. This is as a result of the elastic and resource pooling benefit of cloud computing. A malicious user can employ data recovery techniques to obtain data of a previous user [12]. It is also important to dispose storage devices properly and the process of data backup protected from unauthorized access [12].

3) Web Applications and Application Programming Issues

Applications provided by the CSP are available for access by many users almost at the same time and such accesses have severe implications. The Open Web Applications Security Project in 2013 identified the following security risks. [11, 16]

a. Injection [SQL, OS, and OLAP].
b. Broken authentication and session management.
c. Cross-site scripting.
d. Insecure direct object references.
e. Security misconfigurations.
f. Sensitive data exposure.
g. Missing function level access control.
h. Cross-site request forgery.
i. Using unknown vulnerable components.
j. Invalidated redirect and forwards.

B. Identify Management and Access Control

In a cloud computing environment, the confidentiality, integrity and availability of data is closely linked to the identity management process. There are several users on the cloud from different enterprises, carrying out various activities. Being able to ascertain and manage identity becomes cumbersome and could lead to unauthorized access. Several security issues can be associated with weak identity management and access control. They include: [23]

a. Denial of service by account lock-out.
b. Weak credential reset mechanism.
c. Insufficient authorisation checks.
d. Cross-domain authentication.
e. Insufficient logging and monitoring possibilities.
f. Weakness of extensible access control makeup language.
g. XML wrapping attacks.

Form the discussion so far, it is clear that the security issue on the cloud is wide ranging.

IV. SECURITY CONCERNS FROM INDUSTRY PERSPECTIVE

According to the 2016 Cloud Computing Survey conducted by IDG [9], there were top three concerns with respect to private, public and hybrid clouds. For public cloud; the top three concerns were where data is stored (43%), security of cloud computing solutions (41%) and vendor lock-in (21%), For private cloud; vendor lock-in (24%), lack of skills (22%) and security (21%). For hybrid cloud; security (24%), where data is stored (19%) and lack of skill (18%).

Business leaders are far more concerned about data security both in application and in storage with public cloud, hence many moved their IT environment to the private cloud. In addition, nearly half (46%) of companies say the leading issue they need to resolve before they can fully embrace cloud is that cloud service provider's security meets their compliance requirements.

Similarly in the 2017 Cloud Migration Survey report from Amazon Web Services [22], security and compliance was among the top considerations for choosing target cloud platform. In 2016, the top considerations were reliability (22%), high availability (20%), and security and compliance (17%). In 2017, the top three considerations were price (18%), security and compliance (17%), and reliability (17%). Also a new cloud malware strain called CloudFanta has been compromising users in Brazil and it is expected to spread beyond South America. Most dangerous and most recent is the Ransomware. Ransomware is a type of malicious software that carries out cryptoviral extortion attack, which blocks access to data until a ransom is paid and displays a message requesting payment to unlock it. To prevent being a victim it is imperative to back up all important data.

A. *Industry Solutions*

1) *Scaling and segmentation Protection*. [19]

Cloud computing facilitates agile development and delivery of highly scalable applications, which requires trust of users by ensuring confidentiality and data privacy. Security requires adaptability to scale up with cloud infrastructure itself and to grant protection without decelerating business. IT efficiencies are acquired by pulling together storage, network, and compute resources, and with the help of technologies such as visualization and software-defined networking, entire data centres are being consolidated. To reduce severe potential for loss and damage, organizations ought to isolate business applications and units. Networks need to be sensibly separated into functional security zones to regulate traffic. In terms of elastic security, today's cloud environment require concrete firewalls that provide network security protection at the edge of private clouds and exceptionally scalable north-south data centre firewall. They also require virtual firewalls that implement north-south protection for public clouds. The following scaling and segmentation protections are essential. [19]

a. Private cloud scaling protection automates service insertion and chaining of security appliances in virtual and software defined networks. It also auto-provisions firewalls and security rules to new web and application instances.
b. Public cloud scaling protection auto scales network security with elastic workloads, while auto-provisioning firewall and security rules to new web and application instances.
c. Hybrid cloud scaling protection provides site-to–site VPN connectivity to migrate workloads to provider clouds, as well as remote VPN access to administer workload in the cloud.
d. End–to–end separation delivers deep visibility into traffic that moves east-west over distributed networks, reduce the dissemination of malware, and gives the go-ahead for the isolation and identification of infected devices. A vigorous end-to-end separation strategy includes internal separate firewalling over data centers.
e. Private cloud segmentation isolates applications and data in increasingly consolidated environment. Organization could consider a micro segmentation strategy of fire walling workloads regardless of physical network topology, down to a single virtual workload.
f. Public cloud segmentation isolate applications and workloads while ensuring privacy and compliance in hosted provider environment.
g. Hybrid cloud segmentation targets the persistent connection between private and public clouds and inspects the traffic between them.

It is not sufficient to discover bad traffic and impede malware using diverse devices. Security should be incorporated in public and private cloud with the ability to manage changes to posture accordingly in response to episodes and events. Solutions ought to be erected on an extensible platform with programmatic application programming interface such as JavaScript Object Notation (JSON) and Representational State Transfer (REST), and additional interfaces to interface with hypervisors, clouds, orchestration tools and software-defined networking controllers [19]. This allows for security that dynamically adapts to the growing network architecture and the evolving threat landscape.

2) *Identity and Access Management*

Secure and control access to privileged account is essential. It is important to know how many privileged accounts are available in an enterprise and those to access them [23]. The privileged accounts must be stored securely with encryption and multiple layers of authentication. Also, it is essential to implement a password request process. A privileged password safe can be used for this process. It is also important to implement the least privileged right. An enterprise must determine the level of access based on what an individual should access because this limits malicious actions. A third party solution may sometimes be required for this purpose. Auditing the privileged –access with monitoring and logging is necessary because it is crucial to know what people are doing. An enterprise must determine who has access, when and what system was accessed. The enterprise must know which system has personally identifiable information (PII), health insurance portability and accountability act (HIPAA), who access them and what was done with the information [23]. It is also important to know which system denied access to whom and the commands run on such system. Creating a privileged account management will help to mitigate security issues such as denial of service, insider misuse, zero day, phishing and malware. A 451 Research on security commissioned by Sales Force focused on cloud security. The top 2 challenges that are most critical to address to encourage broader adoption of cloud application and enable hybrid cloud security adoption was an issue. In addition, maintaining consistent access security and authorization controls for cloud application including authentication and authorization was also considered important. Below are current best practices in identity and access management.

- Authentication: Cloud computing authentication involves the verification of users and systems. This involves verifying access request to the information served by another service.
- Authorisation: Upon success of the authentication process, the process of determining the privileges would be given to legitimate system users.
- Auditing: This is the process of reviewing and examining the authorization and authentication records in a bid to check for compliances with predefined security standards and policies.

B. *Top Trends in Cloud Computing Security*

Cloud computing requires a differing approach from the traditional IT security. Cloud computing security requires in depth knowledge of certain nuances and challenges unique to working in the cloud [24]. Without a complete, wholesome security plan geared towards the unique properties of the cloud, an organisation is at risk of losing time and resources

TABLE I
COMPARATIVE ANALYSIS OF CORE CLOUD SECURITY AREAS

References	Virtualization issue	Data storage issue	Web Applications	Application Programming Issues	Identity Management and Access Control	Security Concerns
Ali, M.; Khan, S.U.; Vasilakos, A.V. (2015)	x	x	x	x	x	x
Khan, M.A. (2016)	x	x		x		x
Backe, A; Linden, H. (2015)	x	x			x	
Verma, A.; Kaushal, S. (2011)		x			x	
Singh, S.; Jeong, Y.; Park, J.H. (2016)		x	x	x		x
Shaikh, R.; Sasikumar, M. (2015)		x			x	
Shahzad, F. (2014)	x					x
Subashini, S.; Kavitha, V. (2011)	x		x		x	x
Modi, C.; Patel, D.; Borisaniya, B.; Patel, A.; Rajarajan, M. (2013)	x	x		x	x	x
Arora, R.; Anshu P. (2013)						x
Aldossary, S.; Allen, W. (2016)	x	x			x	
Handa, K.; Singh, U. (2015						x
Singla, S; Singh, J. (2013)		x			x	
Asesh, A. (2015)						x
Chouhan, P.K.; Yao, F.; Sezer, S. (2015)	x	x	x	x	x	
Sailaja, K; Usharani, M. (2017)		x				
Deokar, A. (2017)					x	
Wu, C.; Liu, Q.; Li, Y.; Cheng, Q.; Zhou, H. (2017)	x	x		x	x	
Katsikas, S.K.; (2017) SEPRICC:						x
Kaur, M.; Ghumman, N. (2017)						x
Qadiree, J.; Maqbool, M.I. (2016)		x				
Kumar, S.; Goudar, R.H. (2012)	x					x
Hepsiba, C.L.; Sathiaseelan, J.G.R. (2016)		x				

by exposing its deployment to vulnerabilities that could be identified and mitigated with the right tools. Cloud computing pride itself for cost reduction and better efficiency. An uninformed approach to cloud security can jeopardize the anticipated gains of migrating to the cloud. [24]

- Trusted computing: This is a technology developed to tackle the issues of un-trusted execution environment. Ensuring confidentiality and integrity of data stored in the cloud can be achieved either through sealed when accessing data.
- Information centric security (ICS): One way of achieving ICS would be the introduction of Policy-based or Role-based access controls. These policy or role based access controls can be defined in a language like Extensible Access Control Markup Language (XACML) which governs context-based access rules in policy enforcement point of the data.

V. ANALYSIS AND DISCUSSION

Security concerns in cloud computing is a critical issue. There are several means by which security can be compromised, hence organisations and individuals alike are usually agitated by security on the cloud. No organisation or individual is willing to allow compromise of their data or activities on the cloud. In view of this, security has focused on several important areas in terms of cloud computing. However, this paper selected 6 core cloud computing areas vital to cloud security for analysis. As shown in Table 1, the areas are virtualisation, data storage, web application, application programming interface, identity management and general security concerns. Generally, [16][13][20] covered all the areas under consideration, while [27][29][31][33][34][36][37][38][40] mentioned only of the core security areas being considered. Virtualisation issues was discussed by over 43% of the papers examined. Data storage as it relates to cloud security was examined by 60% of the papers reviewed. Security on the cloud in terms of web application was discussed by 17% of the references. Application programming security concerns was considered by 26% of the papers examined. Another important aspect of security on the cloud which is identity management and access control was discussed by about 50% of the literature reviewed. Finally, general security concerns was discussed by almost 50% of the papers examined.

From the foregoing, despite serious concerns for security on the cloud, not all the core areas being considered in this work received full consideration by the papers reviewed. It is not surprising however that security in terms of data storage received the highest consideration. On the other hand, issues such as virtualisation and identity management were expected to have been discussed the same way as data storage, but this was not the case. Due to the high inherent risk in web application and application programming interface, it was expected that these issues received more attention, again it was not so. In addition, only 39% of the papers reviewed discussed more than 50% of the core cloud security areas selected for analysis. Therefore, a lot more still needs to be done in terms of security considerations in cloud computing. Certainly a lot of research is being undertaken in the area of cloud security, but it is obvious that research work must continue in a bid to keep looking for cloud security solutions to forestall emerging threats. From this research work, it is imperative that the tempo must be sustained in terms of security considerations for web applications and application programming interface.

VI. Conclusion

Cloud computing provides scalable, on demand, elastic, multi-tenant and virtualized services to customers over the Internet through cloud providers. The service types are the SaaS that provides applications, PaaS that provide platform for application development, and IaaS that provides storages and computing infrastructure to users. These services are provided on the basis of service level agreements between the CSP and the user. The SLA specifies the terms of the services provided for a mutually beneficial transaction between both parties. In this paper, a survey of recent developmental trends and issues in cloud SLA negotiations were presented. The paper concluded with a review of SLAs for major CSPs such as Amazon, Microsoft and Rackspace which provide IaaS and PaaS services to clients was then done.

ACKNOWLEDGMENTS

We acknowledge the support and sponsorship provided by Covenant University through the Centre for Research, Innovation and Discovery (CUCRID).

References

[1] Mell, P., Grance, T.: The NIST Definition of Cloud Computing. NIST Special Publication 800-145 (2011)
[2] Khan, N., Al-Yasiri A.: Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework", The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies (IoTNAT' 2016). (2016)
[3] DeChaves, S.A., Westphall, C.B., Westphall, C.M., Gerônimo, G.A.: Customer Security Concerns in Cloud Computing. IARIA, 978-1-61208-113-7 (2011)
[4] Umer, M.F., Sher,M., Khan,I.: Towards Multi-Stage Intrusion Detection using IP Flow Records. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 10 (2016)
[5] Fortinet.: Defining Security for Today's Cloud Environments. www.fortinet.com(2016)
[6] Khan, M.A.: A Survey of Security Issues for Cloud Computing. Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2016.05.010. (2016)
[7] Turab, N.M., Taleb, A.A., Masadeh, S.R.:Cloud Computing Challenges and Solutions. International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.5, September 2013 DOI: 10.5121/ijcnc.2013.5515 209 (2013)
[8] Backe, A., Lindén, H.: Cloud Computing Security: A Systematic Literature Review. Uppsala University Department of informatics and media. (2015)
[9] IDG Executive Summary. Cloud Computing Survey. (2016)
[10] Raoa, R.V., Selvamanib K.: Data Security Challenges and Its Solutions in Cloud Computing. International Conference on Intelligent Computing, Communication &Convergence (ICCC-2015). (2015)
[11] Singh, S., Jeong, Y., Park, J.H.: A Survey on Cloud Computing Security: Issues, Threats and Solution. Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2016.09.002. (2016)
[12] CommVault.: Your Top 5 Cloud Data Protection Challenges. Solved. commvault.com/cloud. (2015)
[13] Shahzada, F.: State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions. The 6th International Symposium on Applications of Ad hoc and Sensor Networks (AASNET'14) (2014)
[14] Rao, V.R., Selvamani K.: Data Security Challenges and Its Solutions in Cloud Computing. International Conference on Intelligent Computing, Communication &Convergence (ICCC-2014) (2014)
[15] An Y. Z., Zaaba Z.F., Samsudin, N.F.: Reviews on Security Issues and Challenges in Cloud Computing. International Engineering Research and Innovation Symposium (IRIS), IOP Conf. Series: Materials Science and Engineering 160 (2016) 012106. (2016)
[16] Ali, M., Khan, S.U., Vasilakos, A.V.: Security in Cloud Computing: Opportunities and Challenges. Information Sciences 305 (2015) 357-383 (2015)
[17] 17. Shaikha, R., Sasikumarb M.: Data Classification for Achieving Security in Cloud Computing. Procedia Computer Science 45 (2015) 493 – 498 (2015)
[18] Rasheed, H.: Data and Infrastructure Security Auditing in Cloud Computing Environment", International Journal of Management 34 (2014) 363-368 (2014)
[19] Ryan, M.D.: Cloud Computing Security: The Scientific Challenge, and a Survey of Solutions. The Journal of Systems and Software 86 (2013) 2263-2268 (2012)
[20] Chang, V., Kuo, Y., Ramachandran, M.: Cloud Computing Adoption Framework: A Security Framework for Business Clouds. Future Generation Computer Systems 57 (2016) 24-41 (2016)
[21] Verma A., Kaushal, S.: Cloud Computing Security Issues and Challenges: A Survey", A. Abraham et al. (Eds.): ACC 2011, Part IV, CCIS 193, pp. 445–454, 2011. © Springer-Verlag Berlin Heidelberg 2011 (2011)
[22] 2017 Cloud Migration Survey Report.: The Most Up-to-Date Benchmarks, Trends, and Best Practices. Amazon Web Services. (2017)
[23] Fallon, M.: Identity and Access Management. Quest Software (2015)
[24] Data Center Journal (2017). Top security trends for 2016[online]. Available: http://www.datacenterjournal.com/top-cloud-security-trends-for-2016/
[25] Subashini, S.; Kavitha, V. A: Survey on Security Issues in Service Delivery Models of Cloud Computing: Journal of Network and Computer Applications 34 (2011) 1-11
[26] Modi, C.; Patel, D.; Borisaniya, B.; Patel, A.; Rajarajan, M. A: Survey on Security Issues and Solutions at Different Layers of Cloud Computing: The Journal of Supercomputing 63(2) (2013) 561-592
[27] Arora, R.; Anshu P.: Secure User Data in Cloud Computing Using Encryption Algorithms: International Journal of Engineering Research and Applications (2013)
[28] Aldossary, S.; Allen, W.: Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions: International Journal of Advanced Computer Science and Applications 7 (4) (2016) 485-498
[29] Handa, K.; Singh, U.: Data Security in Cloud Computing Using Encryption and Steganography: International Journal of Computer Science and Mobile Computing 4 (5) (2015) 786-791
[30] Singla, S; Singh, J.: Cloud Data Security using Authentication and Encryption Technique: International Journal of Advanced Research in Computer Engineering and Technology 2 (7) (2013) 2232-2235
[31] Asesh, A.: Encryption Technique for a Trusted Cloud Computing Environment: IOSR Journal of Computer Engineering 17 (1) (2015) 53-60
[32] Chouhan, P.K.; Yao, F.; Sezer, S.: Software as a Service: Understanding Security Issues: Science and Information Conference (2015) July 28-30 London, UK.
[33] Sailaja, K.; Usharani, M.: Cloud Computing Security Issues, Challenges and its Solutions in Financial Sectors: International Journal of Advanced Scientific Technologies, Engineering and Management Sciences 3 (1)(2017) 190-196
[34] Deokar, A.: Cloud Computing Security Issues, Challenges and Solution: International Journal of Innovative Research in Computer and Communication Engineering 5 (2) (2017) 2549 -2555
[35] Wu, C.; Liu, Q.; Li, Y.; Cheng, Q.; Zhou, H. A Survey on Cloud Security: ZTE Communications 15 (2) (2017) 42-47
[36] Katsikas, S.K.: SEPRICC: Security and Privacy in Cloud Computing: Eighth International Conference on Cloud Computing, GRIDs and Virtualization (2017)

[37] Kaur, M.; Ghumman, N.: Overview of Cloud Computing Security with Issues and Challenges: Journal of Engineering Technologies and Innovative Research 4 (3) (2017) 71-74

[38] Qadiree, J.; Maqbool, M.I.: Solutions of Cloud Computing Security Issues: International Journal of Computer Science Trends and Technology 4 (2) (2016) 38-42

[39] Kumar, S.; Goudar, R.H.: Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: International Journal of Future Computer and Communication 1 (4) (2012) 356-360

[40] Hepsiba, C.L.; Sathiaseelan, J.G.R.: Security Issues in Service Models of Cloud Computing: International Journal of Communication Science and Mobile Computing 5 (3) (2016) 610-615