Journal of Theoretical and Applied Information Technology
10th May 2015. Vol.75. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STATE OF THE ART SURVEY ON SECURITY ISSUE IN CLOUD COMPUTING ARCHITECTURES, APPROACHES AND METHODS

[1]YOUSRA ABDUL ALSAHIB S.ALDEEN, [2]MAZLEENA SALLEH AND [3]MOHAMMAD ABDUR RAZZAQUE

Faculty of Computing, University Technology Malaysia,

81310 UTM Skudai, Johor, Malaysia.

E-mail: yohrmz_8@yahoo.com , mazleena@fc.utm.my, marazzaque@utm.my

ABSTRACT

The development of cloud computing has revolutionized in how the computing and storage are utilized remotely. It has grown from being hopeful business concept to one of the fast growing segments of the IT manufacturing. It has become attractive to businesses and organizations. Although of all the benefits of the cloud, enterprise customers are still unwilling to position their business in the cloud. Security and privacy are the main issues which decrease the growth of cloud computing and preservation of data continue to plague the market. In this paper, we present the vulnerabilities and attacks; identify relevant solution directives to strengthen security in the cloud environment. The main goal of this paper is to offer a better understanding of the security challenges of cloud computing and identify architecture, approaches and methods that have been proposed.

Keywords: *cloud computing, cloud security, characteristics of cloud computing, security challenges, security vulnerabilities*

1. INTRODUCTION

Cloud computing has become as a popular and worldwide paradigm due to enable customers to use computational resources such as software, storage, and processing capabilities related to other companies. Cloud computing is often likened to many like technologies namely: grid computing, utility computing and autonomic computing. Actually, cloud influences several features of these technologies but differs in many features. In a nut shell, cloud computing implements virtualization technology to attain the goal of providing computing resources as a utility [1]. Cloud exploits virtualization techniques in order to offer an effective way of dispatching resources on the minute.

This permits organizing pay-per-use commercial model, meaning that customers can get to exactly choose whatever resources (CPU, memory, bandwidth, security policies, platforms, and hardware load) that are they need, reducing costs by paying only for what is subscribed to [2]. Cloud computing does not realize the dream of computing as a utility only, but offers opportunity for its adoption[1]. But there are challenges faced this new technology. Security and privacy issues are considered the major challenges in cloud computing. In fact, major clients might grip back, choosing to keep infrastructures on-premises rather than moving them to outsourced locations. As the sensitive applications and data are moved into the cloud data centers, run on virtual computing resources in the form of virtual machine. This unique attributes, however, poses many novel tangible and intangible security and privacy challenges. It might be difficult to track the security issue in cloud computing environments [3].

1.1 Characteristics Of Cloud Computing

According to NIST definition which is "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." It can be defined cloud computing by the national institute of standards and technology (NIST, 2009) as having key characteristics, specific delivery

Journal of Theoretical and Applied Information Technology
10th May 2015. Vol.75. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

models, and deployment models as shown in Figure 1.

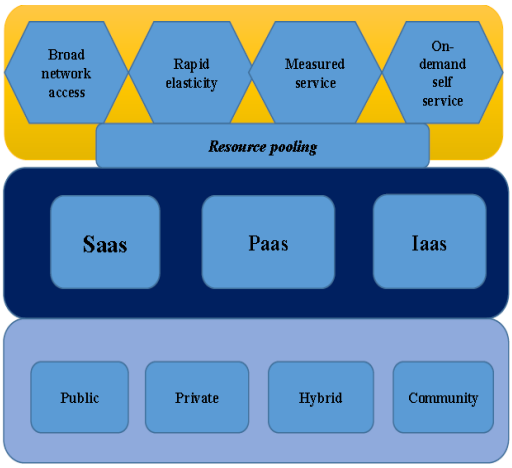

Figure.1 Cloud Computing

There are five essential characteristics of cloud computing that prove their similarities and differences from traditional computing approaches [1].

- Resource pooling: The provider's computing resources are pooled to help numerous consumers using a multitenant model with different physical and virtual resources dynamically allocated and reallocated according to customer demand.
- Rapid elasticity: Capabilities could be fast and elastically provisioned in some cases automatically to quickly scale out; and rapidly released to quickly scale in.
- Measured service: Resource usage can be checked, controlled, and reported providing transparency for both the provider and consumer of the service.
- On-demand self-service: A customer could unilaterally provision computing capabilities such as server time and network storage as needed automatically without needful human interaction with a service provider.
- Broad network access: Capabilities are available over the network and retrieved through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud-based software services.

The main goal of this paper is a comprehensive systematic survey on the cloud security topic, for the most part on security issues. Compare to previous studies, our effort is directed to deliver a more complete and systematic analysis of the research literature. Researches on cloud security issues are either presented as general studies, but within a discussion connected with security, or linked to the security issues that are defined in the respective section. Moreover, a classification of current security studies in cloud environments is introduced in this paper, so this paper classifies current solutions for security issues in cloud environments as architectures, approaches and methods, and the advantages and disadvantages of current studies are tabulated. The analysis of the numerous current security issue studies in the survey delivers the means to also discuss open research challenges and recommend future research guidelines on the subject at the end of this paper.

The rest of this paper is arranged as follows: The section 2 presents security challenges in cloud computing, and their existing solutions. The section 3 presents the research gap. The final section 4 is discussed the conclusion.

2. SECURITY CHALLENGES IN CLOUD COMPUTING

Cloud computing becomes an attractive and popular business model due to its aspects. Furthermore to the benefits at hand, the previous characteristics also result in serious cloud-specific security issues. Security issues have been the control barrier of the growth and extensive use of cloud computing. The major challenges for construction a secure and trustworthy cloud system:

- Outsourcing: it means that users physically lose control on their data and tasks. One of the root causes of cloud insecurity is the loss of control problem. To solve outsourcing security issues, it should be the cloud provider shall be trustworthy by offering trust and secure computing and data storage and the outsourced data and computation shall be confirmable to clienteles in terms of confidentiality, integrity, and other security services.
- Multi-tenancy: it means that the cloud platform is shared and exploited by

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

numerous customers. Furthermore, in a virtualized environment, data related to different clienteles may be located on the same physical machine by certain resource allocation policy.

- Massive data and intense computation: cloud computing is able to handle mass data storage and intense computing tasks. Consequently, traditional security devices may not suffice due to unbearable computation or communication overhead.

This section is classified into four subsections to focus on security issue in cloud environment and present several papers that searched in this space.

2.1 Security Vulnerabilities And Attacks In Cloud Computing

The data storage and processing are provided by cloud providers without control of clients. [4][5] presented Service Level Agreements(SLA's) of cloud computing including problem management ,description of services, performance, , customer obligations and their responsibilities, disaster recovery , security and warranties. An analysis of the multiple security risks that are posed a risk to the cloud has identified by [6][7][8] such as network penetration, packet analysis session and access control faults etc. They also presented the key security fundamentals having data locality, network security, data segregation, data security, web application security, data integrity, data access, tenant, authentication and authorization, data confidentiality, availability, data breaches virtualization vulnerability, identity and backup management and log-on process. [9] have focused on five aspects confidentiality, availability, control, data integrity and audit for security.

Important security challenges should be focused while using cloud services, [10][11][12] such as multi-tenancy issue, resource location, system monitoring and logs, authentication and trust of acquired information and cloud standards. Cloud computing must have central components of the accountability such as responsibility, transparency, remediation and assurance. [13][14] have considered the storage, networks, and virtualization are the core security anxieties in cloud computing. Virtualization lets many clients to part a physical server that lead to the main worries for cloud clients. They have focused to understand what vulnerabilities such as insecure interfaces and APIs cloud; data-related vulnerabilities exist in cloud computing etc. They presented a relationship between vulnerabilities and threats to classify which vulnerabilities lead to the execution of these threats and to create the strong system. Various threats of security issues are discussed by [15][16][17] as insufficiency in security providers, availability ,attacks by other clients, and reliability issues,, wrapping attack, flooding attack which are associated with the cloud computing and analysed the possible security solutions such as mirage image management system, client based privacy manager, flooding attack problem and wrapping attack problem.

The security threats including side channel attacks, Denial of Service (DoS) attacks, man-in-the-middle cryptographic attacks, authentication attacks and Inside-job. have been discussed by [18]. They focused in benefits of using digital ID's. The employee can used digital ID's to access the cloud computing services. It considers the best way to limit the unauthorized access, and also to solve denial issues. Occasionally, a digital ID is called a digital certificate. It is a file on customer's computer that authorized him. [1] discussed the five essential characteristics of cloud computing, three cloud service models, and four cloud deployment models. They discovered the security measures adopted by the largest cloud service provider (Amazon Web Services or AWS) counting their infrastructure security and security best practices followed by AWS.

2.2 Architecture For Solving Security Issue In Cloud

An innovative architecture which is called Advanced Cloud Protection System (ACPS) to protect cloud has been planned by [19]. It could observe both guest integrity and middleware. It could protect them from many types of attack while transparent remains to the service client and to the service providers. It proved able to locally resist to security broken as well as capable of informing the security management layer of such events. Numerous possible architectures and models for random computations and outsourcing data that offer integrity, verifiability, as well as confidentiality are presented by [20]. Their model contains two architectures. The first one calculates the task within a tamper-proof hardware token as well as the other is depends on completely homomorphic encryption. The core technique used in their study is a third architecture which benefits

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

from the features of the previous architectures and cope their particular drawbacks.

A reliable third party that ensures specific security features in cloud have been proposed by [21]. Their solution is named cryptography, precisely public key infrastructure. It is able to ensure the integrity, confidentiality, and authentication of complicated data and communications. [22] have discussed the integrity protection problem in the clouds as well as created a novel architecture that is called Transparent Cloud Protection System (TCPS) to improve cloud security. Their method is a middleware whose central is situated between the virtualization layer and the Kernel. The host can monitor guest VMs and infrastructure mechanisms. Therefore, it is able to preserve the integrity of guest VMs and of the distributed computing middleware. Dynamic migration architecture, leveraging the dynamic provisioning capability of a cloud, to detect and avoid a novel form of DOS attack in a cloud, and confirmed that such an attack could be approved out in a real cloud data center has proposed by [23]. They proposed a novel available bandwidth estimation tool that works accurately and reliably in high-speed networks.

A secured framework for cloud computing depends on the security solutions have been proposed by [24]. Secured VPN ensures a secured environment which clients need to reach the providers 'network. This framework make providers check the authentication of user as well as make sure that the clients are genuine and authorized.[25] proposed a system protecting personal information using role-base as well as attributed- base access control models to bound the admission. The users of private cloud scheme could reach their resources. Consequently, this system could improve the security of the cloud and prevent unauthorized users to access. It also offers availability, confidentiality, and integrity.

2.3 Approach For Solving Security Issue In Cloud

A new approach to timing channel control is proposed by [26]. They could employee an approach of provider-compulsory deterministic execution to protect shared cloud from timing channels. Provider-compulsory determinism is able to avoid implementation of timing. Their experiments have shown that their approach might be practical and effective. [27] suggested a new technique to identify application DOS attack using a new constraint-based group testing model. Group testing offers short detection. The performance of this system has proved false positive-negative rate and little detection latency by hypothetical investigation and initial simulation results.

[28] have proposed an anonymous authentication and authorization protocol. They employed anonymous public key certificates join with normal strong authentication and XACML servers. Their protocol ensures complete anonymity and avoids identity theft through employing anonymous identities. They used more CA for issuing anonymous certificates to make their framework flexible enough. Their protocol could be combined with current identity management systems and offer anonymity as a cloud service.

Essential risks are increased by sharing physical infrastructure between mutually distrustful users [29]. They presented several approaches to mitigate this threat. Cloud providers could obscure both the internal construction and the placement policy to confuse an adversary's efforts to residence a virtual machine on the similar physical machine as its target. Other method might emphasis on the side-channel vulnerabilities and used blinding techniques to reduce the facts. They believed their option is the only resistant solution to this problem. Thus is to be required by clienteles with robust privacy necessities. [30] presented data protection scheme with public auditing scheme and some of the unique factors. A public auditing scheme involves four algorithms including sig gen, key gen, gen proof, and verify proof. [31] concentrated on two of the layers which are the data layer and storage layer. In particular, they stated a scheme for secure third party publications of documents in a cloud. Their system includes support effective storage of encrypted sensitive data, store, manage and query huge quantities of data, and support robust authentication.

2.4 Methods For Solving Security Issue In Cloud

For storing and reaching the data securely from the cloud storage, [32] have proposed a method which gives access to user. They exploited the method of elliptic curve cryptography encryption to preserve data files. They also suggested model consists of two parts which are including private data section and shared data section to attain storage and secure reach. Their technique safeguards the privacy and security of data stored on cloud.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Five types of attacks have been stated by [33]. These attacks are denial of service attack, cross virtual machine, malicious insider's attack, side-channel attack, attacks targeting shared memory and phishing attack. They consider the highest threats for the real world cloud application. In order improve a process to identify these attacks, they generated a database based on their experience by counting number of number of packets received ,packets sent, number of packets lost, number of open ports, difference in VM file size, network usage, and CPU usage.

3. THE RESEARCH GAPS

For giving analysis of this literature review for this section, there is clear proof for an interest toward addressing cloud security issues. Through these developments in this field, it is predictable to see more strong methods to resist these threats with the severe necessities of cloud environments. Till now, customers might not have fully experience about the cloud computing technology. Security of cloud issues must be resolved. Many researchers have confirmed that security should be a highest priority. All these previous architecture approaches, methods should be improved to get a strong secure cloud. Table 1 presents the categorization of current studies on cloud security. Table 2 presents pervious and current studies on cloud security as well as it presents their advantages and disadvantages cloud security.

Table 1 Presents The Categorization Of Studies On Cloud Security

References	Security issue	Architecture	Approach	Methods
Kandukuri et al., 2009[4]	√			
Srinivasamurthy *et al*., 2010[5]	√			
Subashini *et al*., 2011[6]	√			
Bisong, 2011[7]	√			
Kulkarni *et al*., 2012[8]	√			
Zhou *et al*., 2010[9]	√			
Rong *et al*., 2013[10]	√			
Mahmood, 2011[11]	√			
Manager, 2013[12]	√			
Hashizume *et al*., 2013[13]	√			
S.Kumar *et al*., 2013[14]	√			
Nirmala, 2013[15]	√			
Challa, 2012[16]	√			
Chhikara, 2013[17]	√			
Seunghwan *et al*., 2012[18]	√			
Shahzad, 2014[1]	√			
Lombardi *et al*., 2011[19]		√		
Sadeghi *et al*., 2010[20]		√		
Mathew, 2012[21]		√		
Mon et al., 2011[22]		√		
Zissis et al., 2012[23]		√		
Lombardi *et al*., 2010[24]		√		
Liu, 2010[25]		√		
Aviram, *et al*., 2010[26]			√	
Varma *et al*., 2012[27]			√	
Khalid *et al*., 2013[28]			√	
Ristenpart *et al*., 2009[29]			√	
Gowrigolla *et al*., 2010[30]			√	
Hamlen, *et al*., 2010[31]			√	
A. Kumar *et al*., 2012[32]				√
Khorshed et al., 2012[33]				√

4. CONCLUSION

Cloud computing can present numerous business advantages to organizations. It can consider as the fifth utility, following water, electricity, gas and telephony grids, is being commonly accepted through businesses. The product of delivering services on-demand is an applied solution for many

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

low- to medium-sized enterprises, mainly lowering general infrastructure costs and augmenting business efficiency. However, there are numerous challenges connected to security and privacy in the Cloud environment. Cloud computing is today conquered by a big number of challenges. As a result of its fast growth and because virtualization is a relatively new technology, a burst of security issues have been exposed and deliberate by both the academia and industry. Consequently, the governments across the globe must regulate some of the privacy and security requirements. During developing this field, it is expected to get more robust methods to cope with the stringent requirements of cloud environments. Till then, customers could not be fully experience the cloud computing technology and cloud security issues must be determined. Numerous researches have proved that security should be a top priority. This paper was discussed the state-of-the-art on cloud security issues. A comprehensive scope analysis of the literature was presented, which included current studies .Each work was studied to highlight its goal and harvest the resources needed to better cover all topics in the security state of cloud environments from numerous viewpoints. Rudimentary concepts related with clouds were also stated so as to better deliver the basis to understand this paper. Furthermore, this paper surveyed numerous vulnerabilities, threats, attacks, and also current solutions to address security issues in cloud. The analysis of the numerous current security issue studies in the survey delivers the means to also discuss open research challenges and recommend future research guidelines on the subject at the end of this paper. This paper could help the cloud service providers and the end-users to discover the weakness in the previous methods and improve them for building strong cloud security.

Table 2 Presents Pervious And Current Studies On Cloud Security As Well As It Presents Their Advantages And Disadvantages Cloud Security

References	Analysis of Security Issue Including Architecture ,Framework, Approach, Method And Survey	Advantages and disadvantages
Kandukuri et al., (2009) and Srinivasamurthy et al,(2010)[4][5].	Highlighted on several security threats and their exiting method ;and presented security issues that have to be included in SLA (service level agreement)	Adv. Identified reasons of cloud security issue
Subashini et al., (2011), Bisong, (2011) and Kulkarni et al., (2012)[6][7][8]	Surveyed different security risks	Adv. Focused on an important security challenges when using cloud services.
Zhou etal.,(2010)[9]	Discussed the security and privacy issues in cloud.	Adv. Focused on five security attributes.
Rong et al.,(2013) , Mahmood,(2011) and Manager, (2013)[10][11][12]	Focused on an important security challenges in cloud, explained privacy issues of cloud computing and identified method of dynamically routing data.	Adv. Provide reader knowledge of security and privacy challenges and at the same time benefits of cloud.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Hashizume et al., (2013) and S. Kumar et al., (2013)[13][14]	Discussed what vulnerabilities exist in Cloud Computing and focused on Virtualization and different types of Virtualization.	Adv. Presented the benefits of knowing virtualization and its effect on security cloud.
Nirmala, (2013), Challa, (2012) and Chhikara ,(2013)[15][16][17]	Presented the exiting solutions such as Client Based Privacy Manager, Mirage Image Management System, Wrapping Attack Problem, and Flooding Attack.	Adv. Presented exiting solutions.
Seunghwan et al,(2012) [18]	Discussed digital ID's that should be used by employee in accessing the cloud computing services.	Adv. Presented the importance of authentication method when accessing cloud computing.
Shahzad, 2014[1]	Discussed the five essential characteristics of cloud computing, three cloud service models, and four cloud deployment models.	Adv. discovered the security measures adopted by the largest cloud service provider.
Lombardi et al., (2011)[19]	Architecture, Proposed advanced cloud protection system (ACPS) for cloud security issue.	Adv. proves it can respond to security breaks. Dis adv. It could not protect cloud system from all attacks.
Sadeghi et al., (2010)[20]	Architecture Combined a trusted hardware token with Secure Function Evaluation (SFE).	Adv. Proposed third architecture that uses the advantages of the previous architectures and overcomes their disadvantages.
Zissis et al., (2012)[23]	Architecture, Proposed solution called upon cryptography.	Adv. Ensures the authentication, integrity and confidentiality of involved data and communications. Dis adv. It is difficult getting trusted third party.
Lombardi et al., (2010)[24]	Architecture, Transparent Cloud Protection System (TCPS).	Adv. focused on the integrity of virtual machines.
Liu, (2010)[25]	Architecture, Proposed and evaluated a new mechanism for applications to dynamically relocate to a different infrastructure when the desired Quality of Service (QoS) could not be met.	Adv. can detect and elude a new form of DOS attack.
Mathew ,(2012)[21]	Framework, proposed a secured framework for cloud computing depending on the security solutions suggested.	Adv. Ensure for user authentication for the approaching of clients.
Mon et al., (2011)[22]	Architecture, Proposed method for limiting access which is attributed- based access control and role-based access control.	Adv. Could enhance the security of the cloud by preventing unauthorized users to access and provide attributes of security.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Aviram, *et al*., (2010)[26]	Approach, A new approach to timing channel control	Adv. It may be practical and efficient.
Varma *et al*., (2012)[27]	Approach, Proposed a new technique to detect DOS attack.	Adv. low latency and false positive/negative ate.
Khalid et al.,(2013)[28]	Approach, Designed an anonymous authentication and authorization protocol.	Adv. Could be integrated with existing identity management systems and provided anonymity as a cloud service.
Ristenpart et al.,(2009)[29]	Approach, presented a number of approaches for mitigating risks arise from sharing physical infrastructure.	Dis adv. It is the only specialized for this problem
Gowrigolla et al., (2010)[30]	Approach, Presented a data protection scheme with public auditing scheme.	Adv. It ensures authentication access.
Hamlen, et al., (2010)[31]	Approach, deal with two layers that are the data layer and storage layer.	Adv. efficient storage and provide strong authentication .
A. Kumar et al.,(2012)[32]	Method, proposed model has two parts in the cloud storage server by exploiting the technique of elliptic curve cryptography encryption.	Adv. Ensure the security and privacy of data stored on cloud
Khorshed et al., (2012)[33]	Method, Generated a database.	Dis adv. Could not detect all attacks

REFERENCES

[1] Shahzad, F. (2014). State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions. *Procedia Computer Science*, *37*, 357–362. doi:10.1016/j.procs.2014.08.053

[2] Fernandes, D. a. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2013). Security issues in cloud environments: a survey. International Journal of Information Security, 13(2), 113–170. doi:10.1007/s10207-013-0208-7

[3] Williams, M. I. (n.d.). New Tool for s Busi ness A Quick Start Guide to Cloud ComputinG.

[4] Kandukuri, B. R., V., R. P., & Rakshit, A. (2009). Cloud Security Issues. 2009 IEEE International Conference on Services Computing, 517–520. doi:10.1109/SCC.2009.845.

[5] Srinivasamurthy, S., Wayne, F., & Liu, D. Q. (2010). Survey on Cloud Computing Security. In *Proc. Conf. on Cloud Computing, ... (2010)*. salsahpc.indiana.edu.

[6] Subashini, S., & Kavitha, V. (2011). Journal of Network and Computer Applications A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11. doi:10.1016/j.jnca.2010.07.006

[7]Bisong, A. (2011). A N OVERVIEW OF THE S ECURITY C ONCERNS IN, *3*(1), 30–45.

[8]Kulkarni, G., Gambhir, J., Patil, T., & Dongare, A. (2012). A security aspects in cloud computing. *2012 IEEE International Conference on Computer Science and Automation Engineering*, 547–550. doi:10.1109/ICSESS.2012.6269525

[9]Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. *2010 Sixth International Conference on Semantics, Knowledge and Grids*, 105–112. doi:10.1109/SKG.2010.19

[10]Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, *39*(1), 47–54. doi:10.1016/j.compeleceng.2012.04.015

[11Mahmood, Z. (2011). Data Location and Security Issues in Cloud Computing. *2011 International Conference on Emerging Intelligent Data and Web Technologies*, 49–54. doi:10.1109/EIDWT.2011.16

[12]Manager, S. (2013). Security Issues And Resource Planning In Cloud Computing 1, *2*(2).

[13]Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Applications, *4*(1), 5. doi:10.1186/1869-0238-4-5

[14]Kumar, S., Pal, S., Kumar, A., & Ali, J. (2013). Virtualization , The Great Thing and Issues in Cloud Computing, 338–341.

[15]Nirmala, V. (2013). Data Confidential lity and Integrity Verif fication using User Aut thenticator scheme in cloud c, 0–4.

[16]Challa, K. A. (2012). Cloud Computing Security Issues with Possible Solutions, *8491*, 340–344.

[17]Chhikara, S. (2013). Analyzing Security Solutions in Cloud Computing, *68*(25), 17–21.

[18]Seunghwan, J., Gelogo, Y. E., & Park, B. (2012). Next Generation Cloud Computing Issues and Solutions, *5*(1), 63–70.

[19] Lombardi, F., & Di Pietro, R. (2011). Secure virtualization for cloud computing. *Journal of Network and Computer Applications*, *34*(4), 1113–1122. doi:10.1016/j.jnca.2010.06.008

[20] Sadeghi, A., Schneider, T., Winandy, M., & Horst, G. (2010). Token-Based Cloud Computing, *2*, 417–429.

[21] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. doi:10.1016/j.future.2010.12.006

[22] Lombardi, F., & Moro, P. A. (2010). Transparent Security for Cloud, 414–415.

[23] Liu, H. (2010). A New Form of DOS Attack in a Cloud. Acm, Pages: 65-75, 15437221(15437221), 65–75. Retrieved from portal.acm.org

[24] Mathew, A. (2012). SECURITY AND PRIVACY ISSUES OF CLOUD COMPUTING ;, *2*(4).

[25] Mon, E. E., & Naing, T. T. (2011). The privacy-aware access control system using attribute-and role-based access control in private cloud. 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, 447–451. doi:10.1109/ICBNMT.2011.6155974

[26] Aviram, A., Hu, S., & Ford, B. (2010). Determinating Timing Channels in Compute Clouds. Computer and Information Science, 1003.5303(15437221), 6.

[27] Varma, P. R. K., & Krishna, D. S. (2012). Application Denial of Service Attacks Detection using Group Testing Based Approach. *International Journal of Computer Science & Communication Networks (2012)*, *2*(2), 167–171. Retrieved from www.doaj.org

[28] Khalid, U., Ghafoor, A., Irum, M., & Shibli, M. A. (2013). Cloud Based Secure and Privacy Enhanced Authentication & Authorization Protocol. Procedia Computer Science, 22, 680–688. doi:10.1016/j.procs.2013.09.149

[29] Ristenpart, T., Tromer, E., & Savage, S. (2009). Hey , You , Get Off of My Cloud : Exploring Information Leakage in Third-Party Compute Clouds.

[30] Gowrigolla, B., Sivaji, S., & Masillamani, M. R. (2010). Design and auditing of Cloud computing security. *2010 Fifth International Conference on Information and Automation for Sustainability*, 292–297. doi:10.1109/ICIAFS.2010.5715676

[31] Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security Issues for Cloud Computing. International Journal of Information Security and Privacy, 4(2), 36–48. doi:10.4018/jisp.2010040103

[32] Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012). Secure storage and access of data in cloud computing. *2012 International Conference on ICT Convergence (ICTC)*, 336–339. doi:10.1109/ICTC.2012.6386854

[33] Khorshed, M. T., Ali, a. B. M. S., & Wasimi, S. a. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, *28*(6), 833–851. doi:10.1016/j.future.2012.01.006