The Journal of Social Sciences Research
ISSN(e): 2411-9458, ISSN(p): 2413-6670
Special Issue. 6, pp: 599-606, 2018
URL: https://arpgweb.com/journal/journal/7/special_issue
DOI: https://doi.org/10.32861/jssr.spi6.599.606

Academic Research Publishing Group

Original Research Open Access

Threats and Vulnerabilities Affecting the Adoption of Cloud Computing in Iraq

Omar Adil Dheyab*
Universiti Pendidikan Sultan Idris, Malaysia

Ahmed Ibrahim Turki
Department of Physics, University of Samarra

B. Rahmatullah
Universiti Pendidikan Sultan Idris,Malaysia

Abstract

Cloud computing offers many benefits including enhanced flexibility, disaster recovery, free capital expenditures, automatic software updates, sustainability, and work anytime, anywhere. In addition, many other features and services can be offered to customers. However, cloud computing still suffers many threats which may cause vulnerabilities. Therefore, today many organizations are still hesitant to adopt cloud computing because of fear for privacy of their data and confidentiality. Understanding and addressing security threats are a prerequisite for unleashing the huge potential of cloud computing. In this study, a survey is conducted on some cloud service providers and users to explore security threats and vulnerabilities in cloud computing experienced by many organizations in Iraq. Consequently, many countermeasures are proposed. Descriptive research methodology is adopted in this research. The results of the study showed that privacy, confidentiality, control of data are the main obstacle to cloud computing adoption.

Keywords: Cloud computing; SPI model; Vulnerabilities; Security threats; Countermeasures.

1. Introduction

Cloud computing is a modern technology which takes up a broad space of discussion in information technology. The National Institute of Standards and Technology (NEST) defines cloud computing as a model that provides convenience, on-demand service, ubiquity, and access to shared resources with minimal administrative effort. Cloud computing increases the ability of companies and organizations to meet customer demands, provides services without the need for software licenses, and it trains or purchases vendors infrastructure. Users use servers (e.g. iCloud, Dropbox,) to access data which are stored anywhere and anytime (Bruno *et al.*, 2017). Despite all the offered services by cloud computing in IT, cloud service providers and customers have an urgent need to understand, analyze and examine all the risks and security issues. Companies are still hesitant to adopt cloud computing entirely in their work, as they are afraid of the privacy and confidentiality of their data or their data fall in the wrong hands. (Keiko *et al.*, 2013). The basic concerns that prevent cloud computing adoption are the privacy of data and security threats. Thus, many researchers do researches on the technical side of cloud computing, to understand, identify and analyze all security threats. Most of these studies are conducted in collaboration with cloud users and service providers to understand security problems and find countermeasures. In this study, the following questions will be are answered:

1. What do organizations in Iraq face threats and vulnerabilities when relying on cloud computing?

2. What are the countermeasures and solutions to such threats in cloud computing as well as vulnerabilities?

Section 2 presents literatures related to cloud computing, and threats as well as vulnerabilities. The research methodology is presented in Section 3. In Section 4, the results of the questionnaire are analyzed. The discussion and conclusion are presented in Section 5. Finally, Section 6 presents recommendations for future work.

2. Literature Review

Day by day the interest in cloud computing is growing in industrial and scientific societies. It is the first of the ten promising technologies that organizations and companies are looking for. The cloud computing market in 2010 reaches about $ 68 billion, and in 2014 it reaches $ 148 billion (Gartner Inc, 2011). Cloud computing enables the use of (networks, services, applications, storage, and servers) on demand, quickly and with minimal administrative effort. It also offers a lot of benefits such as rapid server restructuring, data storage solutions, disaster recovery, scalability and flexibility (Keiko *et al.*, 2013); (Zhang *et al.*, 2010). Cloud service providers are responsible for any breach or degradation of the data, so they have to secure systems out of threats. Companies and organizations are still reluctant to rely on cloud computing (Munir and Palaniappan, 2013). Lack of experience among customers affects data security as well as service availability (Ramgovind *et al.*, 2010). For this reason, threats and weaknesses are identified in research literature. The threat is defined as a potential attack that results in damage to data or resources. The weakness is also referred to as a flaw in the system that makes the possibility of a successful attack

*Corresponding Author

significant (Keiko *et al.*, 2013). The only drawback from the view point of cloud computing is the lack of security. Users and cloud service providers must work together to strengthen security and maintain data and services (Shaikh and Haider, 2011). The two most important aspects that determine the level of vulnerability in a cloud-computing platform is the choice of deployment and delivery model (Modi *et al.*, 2012). General Vulnerabilities, Threats, and Attacks in Cloud computing, like other areas of IT, suffers from several security issues, which need to be addressed (Coppolino *et al.*, 2016; Wang, 2009). Vulnerabilities and open issues Cloud is a set of technology, process, people, and commercial construct. Like all other technology, process, people, and commercial construct, cloud too has vulnerabilities (Ramachandran, 2015; Roundup of Cloud Computing Forecasts and Market Estimates, 2015). Cloud Computing offers a lot of services to both organizations and users, in terms of reducing operating expenses and capital expenditures. However, there are limitations on the use of cloud computing that stand in the way of its total adoption, security is the main concern of organizations and users. (Subramanian and Jeyaraj, 2018). Virtual machines for users can be created, transferred, retrieved, copied, and shared through virtualization, allowing users to run many applications (Jasti *et al.*, 2010). Despite the virtualization features, the additional layer provides new opportunities for attackers, so they must be secured (Owens, 2010). Any defect in the security of the physical device affects the security of the virtual machine so security is the biggest obsession, because it adds more complexity of the link and more entry points (Reuben, 2007). According to Rebecca, linear regression technique was implemented to find out the responses. This recommends awareness campaigns to a particular cloud computing users in relate to cloud data privacy (Rebecca *et al.*, 2016). Resource exhaustion creates denial of service attacks. This can be developed due to poor design, bad utilization of resources on the service side, and leakage of data. It can be monitored by using black box testing method (Sharon *et al.*, 2013). The adoption of cloud computing in business is slowing down due to the threats and vulnerabilities like data loss, vulnerable systems, data breaches, poor authentication and identity management, lacking due to diligence, account hijacking, advanced threats, limited security tools, ransomware, human error, vulnerable IoT devices and the associated vulnerabilities (Suryateja).

From this literature, few current challenges identified with cloud computing security that are related to visualization layers of the cloud computing. To overcome the security issues a security guide is to be initiated to reinforce cloud preparation stage in the cloud adoption network. They believe that this will promote and increase the cloud computing adoption among small and medium organizations (Nabeel and Adil Al-Yasiri, 2016). Discussed the top cloud computing security threats "abuse and nefarious use of cloud computing". The cyber criminals and hackers are already misused cloud computing due to weak registration and some security threats. This research encouraged to conduct more research to get information about the risks and impact of this vulnerabilities on confidential business data; also cloud security providers need to explore and deploy proactive security methods to stop unauthorized and illegal access to business information residing on the cloud (Yasir and Marwan, 2013).

Minimal investment, cost reduction and rapid deployment are main factors that drive industries to utilize Cloud services and allow them to focus on core business concerns and priorities rather than dealing with technical issues (Ponemon, 2011).

2.1. Service Models in Cloud Computing

There are many types of cloud computing services:

2.1.1. Infrastructure as a Service

is the bottom layer of the cloud computing model, which offers (memory, processor, data center, virtual server, storage capacity, network connections) as services provided by the cloud service provider like (Amazon EC2). Infrastructure as a service is a revolution in IT investment (Azzedine Boukerche and Robson, 2018). which helps to allocate virtual and physical resources more flexibly. It also provides provisions and scalability without wasting time and money. Infrastructure as a service also focuses on virtual machine monitor, intrusion detection system, intrusion prevention system, and firewall (Flavio *et al.*, 2011).

2.1.2. Platform as a Service

Many services are provided such as integrated development environments, software, architecture, framework, and development tools. Customers control all their applications as opposed to the infrastructure. The best example of a platform as a service is Google Drive . The platform as a service is more scalable than software as a service (Saurabh *et al.*, 2016).

2.1.3. Software as a Service

Software as a service provides customers with access to applications with the help of an integrated development environment, as well as the possibility of transferring applications and data to storage servers through the software service over the Internet. CRM and Salesforce.com are achieved by users of service software as a service (Ashish and Kakali, 2017).

2.2. Deployment Models

Cloud computing has 4 deployment models for cloud services, according to users' requirements:

2.2.1. Public Cloud

The cloud provider provides and manages the public cloud, where its physical infrastructure is far from the user's geographic location. Cloud resources are shared among many customers. In addition, users pay for the cloud service provider based on the services they use (Ashish and Kakali, 2017); (Muhammad Baqer *et al.*, 2017).

2.2.2. Private Cloud

A cloud is owned by one organization only and its resources are not used by any other users. This organization may own cloud infrastructure or not, but it can run it on its own or through a third party. It is not required to be the same as the geographical location of the organization (Mazhar *et al.*, 2015).

2.2.3. Community Cloud

This type of cloud is managed and controlled by several institutions and organizations. The costs in the private cloud are reduced, as are security concerns in the general cloud. This kind of cloud often exists outside and inside the campus or is shared by more than one organization (Saurabh *et al.*, 2016).

2.2.4. Hybrid Cloud

This kind of cloud is a combination that combines more than one kind of cloud (public, private, community) with the same capabilities and infrastructure (Ashish and Kakali, 2017).

2.3. Cloud Data Security

Cloud computing security faces a growing number of threats for the following reasons. Firstly, there is a large number of users who access important cloud data such as passwords and bank accounts that must be proprietary to the owner. This makes its security vulnerable to attack when making a mistake, even if it is simple. Secondly, cloud computing is rapidly evolving. Traditional security solutions quickly become less useful, and continued reliance on them results in data loss that the end-user no longer has (Ravi Kumar *et al.*, 2017). The use of SaaS poses a major challenge to data security, as the SaaS service provider is responsible for providing security for organizational data. Data backup is a security solution to ensure that data is not lost when a disaster occurs, but this is fraught with other security risks (Ashish and Kakali, 2017; Mazhar *et al.*, 2015).

There is a marked increase in cybercrime. which create a lot of data security issues. At the same time, users of the cloud have no idea how to store their data. For this reason, cloud service providers are responsible for the availability, integrity and confidentiality of data (Ravi Kumar *et al.*, 2017). Security and privacy issues are the most widespread and complex, coinciding with the adoption of organizations on cloud computing and contribute to its spread (Muhammad Baqer *et al.*, 2017). Providing users with accurate details about their identification through the Internet is dangerous as attackers can use it to increase cyber-attacks. To preserve privacy as well as security issues like disaster recovery, operational integrity, and confidentiality, several measures should be taken (Edington and Kishoreb, 2017):

- To avoid known threats and maintain safety standards there must be a strong encryption system.
- Protect critical servers from illegal and unauthorized access by enhancing controls.
- To maintain data confidentiality, the service provider must have limited access to data, which the provider can only manage it.
- To avoid loss of data in case of disaster or infrastructure failure, data backups must be made.

2.4. Threats

The issue of security is important especially with the increasing spread of cloud computing. Cyber-attacks increase with the widespread use of applications (Gururaj *et al.*, 2017). To gain customer confidence, service providers make great efforts to reduce the risk of attacks. For this reason, security issues in cloud computing take a lot of researchers efforts (Minhaj, 2016). Therefore, CSA is a document presented in 2013 which contains the important security threats addressed in this paper. (Anonymous; Choo, 2013).

- Data breaches
- Data loss and leakage
- Insecure APIs
- Hijacking of accounts , services and traffic
- Malicious Insider
- Denial of Service
- Abuse and malicious use of cloud resources
- Shared technological issues
- Identity theft
- Risk profiling

2.5. Vulnerabilities

Vulnerability is an influential factor used by saboteurs to threaten cloud computing. Vulnerability is defined, as exploiting a certain gap in the assets (network, systems, environments, software, etc.) to cause damage or sabotage in the organization (Philipp and Koosha, 2017). Cloud computing has several key vulnerabilities that we present in this section:

- Portability and data protection: A contract between a client and a cloud service provider is the key step for delivering cloud services. Therefore, this contract has a lot of drawbacks, especially after the end of the contract, what is the fate of data saved by the service provider? Is there a guarantee from the provider not to misuse this sensitive data ?. Consequently, data transfer and protection is difficult and complex security issues (Munir and Palaniappan, 2013).
- Availability and Reliability: Cloud computing isn't an ideal technique because it is not ideally available, in addition to its lack of reliability in many cases. Many Internet-based applications and services are therefore affected by cloud infrastructure failures. Cloud service provider is the responsible for this failure (Munir and Palaniappan, 2013).
- Vulnerabilities in Virtual Machines: Cloud services are affected by virtual machine attacks, which result in many vulnerabilities in virtual machines that are hosted. There are several attacks based on virtual machines (covert channels, deallocation of resources and unrestricted allocation, Uncontrolled snapshots, Uncontrolled Migration, Uncontrolled rollback, etc.) (Minhaj, 2016).
- Cryptography: In cloud computing, many cryptographic mechanisms are applied to gaps but often fail and these challenges must be overcome. Discrete algorithm and RSA fail because brute force attack based on faulty implementation and bad password. There are other issues related to cryptography like computation efficiency and poor key management (Saurabh *et al.*, 2016).
- Hijacking and session riding: Is a process of directing the client to a suspicious and phishing web site. This process is done by exploiting software loopholes, phishing, and fraud. These attacks are usually caused by frequent use of the password and credentials. In cloud computing, someone's credentials can be used by the attacker where he can hack an account, redirect the client to wrongful sites, return falsified information, manipulate data, perform data transaction, and capture the activities (Ashish and Kakali, 2017).
- VM escape: hypervisor is exploited by attackers remotely to control infrastructure, but this attack is rare but exists (Minhaj, 2016).
- Cloud service provider lock-in: The cloud service provider must guarantee the user the freedom to move to another provider when needed. The user wants to rely on more than one service provider and not to be forced by the provider. Yet this is difficult because there are no fixed standards (data formats, protocols), which causes termination of service in particular (Michael *et al.*, 2018).
- Denial of service: An attacker controls all possible resources provided to customers by targeting the cloud system. This drives to the cloud system to inability to meet the resources of legitimate users (Luigi *et al.*, 2017).
- Resource exhaustion: Cloud management doesn't have to be restricted to the consumption of available resources (CPU, database, file storage system, and memory) more than required and required by users. The attacker consume at one time more than what is required, which deprives the users of the right to slow down their work and applications in addition to their systems (Ashish and Kakali, 2017).

3. Methodology of Research

In this research, descriptive research methodology is adopted. It presents a literature review on many articles published in conferences and magazines on cloud computing and information technology, available on many databases of global publishing houses (Elsevier, springer, IEEE, etc…). In addition, data are collected through a distributed questionnaire for cloud service providers and many users to know the security issues for cloud computing, through which questions are answered. The study is conducted on six private sector organizations, all located in Baghdad, northern Iraq and adopted on cloud computing. The obtained results in Section 4 are based on quantitative and qualitative analysis of data received from organizations.

4. Research Results

This part of the research presents the results of the questionnaire obtained from cloud service providers and customers. It explores various threats, vulnerabilities and countermeasures. An organized method was used to prepare the questions to obtain the required information. Table 1 presents different views on the benefits of cloud computing for both service providers as well as customers.

Table-1.Benefits of Cloud Computing

Organization	Most Important Benefit of Cloud
Org (1)	Cost savings, Disaster recovery, Flexibility, Consumption-based commercial models
Org (2)	Increased collaboration, Reduced costs, Greater security, Greener solutions
Org (3)	Automatic software updates, Capital-expenditure cuts
Org (4)	IT efficiency, Work from anywhere, Document control
Org (5)	Competitiveness, Environmentally friendly
Org (6)	Increased collaboration; Disaster recovery, Automatic software updates, Loss prevention

Table 2 provides answers from cloud service providers and customers on the obstacles that prevent cloud computing adoption. The results of the survey show that privacy and data control are obstacles, which prevent the adoption of cloud computing technology. Security threats and risks come in second place with 70%. Organizations are asked to rank threats on the basis of severity, the results indicate that data breaches and theft constitute a major obstacles and concerns to organizations. The results also show that organizations are less concerned about identity theft and risk profiling.

Table-2. The Biggest Obstacles to Cloud Computing Adoption

Organization	1st obstacle	2nd obstacle	3rd obstacle	4th obstacle
Organization (1)	privacy and data control	Security threats and risks	Regulatory compliance	Data Auditability
Organization (2)	privacy and data control	Security threats and risks	Regulatory compliance	Availability
Organization (3)	privacy and data control	Security threats and risks	Geographic proximity	Authentication
Organization (4)	privacy and data control	Geographic proximity	Data Confidentiality	Software Licensing
Organization (5)	privacy and data control	Security threats and risks	Geographic proximity	Availability
Organization (6)	privacy and data control	Data Lock-In	Performance Unpredictability	Scalable Storage

Table 3 shows various security threats

Table-3. The Main Security Threats in Cloud Computing

	Threats /Organization	Org(1)	Org(2)	Org(3)	Org(4)	Org(5)	Org(6)
T1	Data breaches	2	2	1	2	3	2
T2	Data loss and leakage	3	3	2	3	3	5
T3	Insecure APIs	2	4	4	4	7	5
T4	Hijacking of accounts, services and traffic	5	6	5	8	4	3
T5	Malicious Insider	2	3	7	8	6	4
T6	Denial of Service	7	6	8	7	9	4
T7	Abuse and malicious use of cloud resources	8	8	7	6	10	4
T8	Shared technological issues	9	8	8	7	8	7
T9	Identity theft	10	9	10	8	9	10
T10	Risk profiling	10	10	9	10	10	9

Table 4 shows the results of the classification of cloud computing users for vulnerabilities in cloud computing, especially in security.

Table-4. The Results of The Classification of Cloud Computing Users

#	Vulnerabilities/Organization	Org(3)	Org(4)	Org(5)	Org(6)
V1	Portability and data protection	2	4	3	2
V2	Availability of service and Reliability	3	5	5	3
V3	Vulnerabilities in Virtual Machines	4	4	6	5
V4	Cryptography	5	6	5	5
V5	Hijacking and Session riding	5	7	6	4
V6	VM escape	9	8	9	8
V7	Cloud service provider lock-in	8	6	9	7
V8	DoS attack	8	7	4	4
V9	Resource exhaustion	9	8	6	9

Table 5 shows the security countermeasures followed by the cloud service providers surveyed. These countermeasures are used to add a high level of security before providing users with cloud services.

Table-5.The Responses of Organizations

Threats	Countermeasures	
	Organization (1)	**Organization (2)**
Data breaches	Encrypt Sensitive and confidential information	Increase security awareness
Data loss and leakage	Digital signatures and FRS techniques	Backup mechanisms and Homomorphic encryption
Insecure APIs	Encrypting transferred data, authentication mechanism,	Dynamic credentials and Secure Authentication, Web application scanners
Hijacking of services, accounts and traffic	Use strong authentication mechanisms, secure communication channel, security policies	Access and Identity management guidance and Dynamic credentials
Malicious Insider	Strong malware protection.	Use agreement breach notifications, reporting and security
Denial of Service	Provide limited accounting resources by service providers	Network monitoring
Abuse and malicious use of cloud resources	Provide robust registration, monitor the network status, and technique of authentication	Monitor data traffic and user behaviors
Shared technological issues	Use of access control mechanisms and strong authentication of administrative tasks	Prevent customers from sharing information between them through the use of segregation control panels
Identity theft	Use robust complex passwords	Use potent authentication mechanisms
Risk profiling	alter system	Secure data by monitoring logs, data, and infrastructure

5. Discussion

Cloud computing technology includes all components (infrastructure, access management systems, networks, and end-user machines). To achieve cloud security, infrastructure and data must be protected from all types of attacks and threats (Khalil *et al.*, 2014). In this research, many threats as well as vulnerabilities are addressed and analyzed for a specific period. Cloud users and providers have identified several threats and vulnerabilities, including privacy, data control, security threats and risk that make them reluctant to rely on cloud computing. The big drawback of cloud computing is security. In which customers and cloud service providers work together to ensure a secure cloud infrastructure. Organizations have identified many threats through the questionnaire such as data breaches, data loss, denial of service, account hijacking and others. However, data breaches is the most important compared to identity theft and risk profiling is less important. As a result, users are concerned about their data, how they are stored, controlled, and secured when they use different models of clouds. These concerns and vulnerabilities cause legal and financial issues for organizations (Subashini and Kavitha, 2011). In terms of vulnerabilities, many cloud users surveys indicate that data protection, availability, reliability, and attacks on the virtual machine are important vulnerabilities they had to avoid and be careful about it. For this reason, studies and statistics must be publicized in order to ensure reliability at work. In addition, the participation of this type of information and statistics helps the concerned organizations to understand and analyze these threats and vulnerabilities, thus contributing to data protection from new and potential attacks (Khalil *et al.*, 2014).

Service providers are directly responsible for cloud security, so they must provide countermeasures and appropriate security solutions to various threats, attacks and vulnerabilities. Such countermeasures and solutions must be dynamic and freelance. In addition, these solutions must be continuously updated with the modernization and, development of the infrastructure and services provided. Before the start of any project, the cloud service providers also share the security requirements and check them through a test phase and review them continuously even after the completion of the project (Keiko *et al.*, 2013).

6. Conclusion

Cloud service providers in Table 5 list the important countermeasures to monitor report and address security threats. For example, data breach countermeasures are to encrypt sensitive and confidential information as well as to increase security awareness, making them safe when stored in the cloud. Digital signatures, FRS techniques, Backup mechanisms and Homomorphic encryption can be used as countermeasures for data loss and leakage. The results of this study show the important threats and vulnerabilities faced by organizations in Iraq, which are an obstacle to the adoption of cloud computing completely. Statistics show that there is a real fear by these organizations about the privacy of data or loss and falling in the wrong hands. Therefore, such technical problems open the door for researchers to provide further research and technical solutions, in cooperation with service providers and end users.

6.1. Limitations and Future Work

This research has been somewhat restricted in terms of sample size and time, since the results cannot be considered a criterion for all countries, organizations and for all cloud models. Access to information is also difficult because of the scarcity of organizations that rely entirely on cloud computing in their work inside Iraq . In addition, organizations are afraid of disclosing the threats and vulnerabilities they suffer from fear of being attacked. For this reason, the names of service providers and users have been kept confidential at their request. In-depth research, studies and analysis of various threats, attacks, challenges and vulnerabilities can be conducted in many areas of cloud computing (such as cloud storage, virtualization, applications, and platforms, etc.) in all cloud computing models and propose solutions and countermeasures.

References

Anonymous: Available: http://www.cloudsecurityalliance.org

Ashish, S. and Kakali, C. (2017). Cloud security issues and challenges, A survey. *Journal of Network and Computer Applications*, 79(2017): 88-115.

Azzedine Boukerche and Robson, E. D. G. (2018). Vehicular cloud computing, Architectures, applications, and mobility. Computer networks. 135.

Bruno, B., Carlos, F., Danilo, S., Dionisio, F. and P., M. (2017). A QoS-driven approach for cloud computing addressing attributes of performance and security. *Future Generation Computer Systems*, 68(2017): 260-74.

Choo, D. (2013). Timetec cloud security, Facing security challenges head-on, academia fingertec.

Coppolino, L., D'Antonio, S., Mazzeo, G. and Romano, L. (2016). Cloud security, Emerging threats and current solutions. *Computers & Electrical Engineering*: Available: https://doi.org/10.1016/j.compeleceng.2016.03.004

Edington, A. M. and Kishoreb, R. (2017). Forensics framework for cloud computing. *Computers & Electrical Engineering*, 60: 193-205.

Flavio, Lombardi, Pietro and RobertoDi (2011). Secure virtualization for cloud computing. *J. Netw. Comput. Appl.*, 34(4): 1113-22.

Gartner Inc (2011). Gartner identifies the Top 10 strategic technologies for 2011. Available: http://www.gartner.com/it/page.jsp?id=1454221

Gururaj, R., Mohsin, I. and Farrukh, A. K. (2017). A comprehensive survey on security in cloud computing.

Jasti, A., Shah, P., Nagaraj, R. and Pendse, R., 2010. "Security in multi-tenancy cloud In." In *IEEE International Carnahan Conference on Security Technology (ICCST), KS,USA. IEEE Computer Society Washington, DC, USA.* pp. 35-41.

Keiko, H., David, R. G., Fernández-Medina, E. and B., E. F. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(5).

Khalil, I. M., Khreishah, A. and Azeem, M. (2014). Cloud computing security, a survey. *Computers*, 3(1): 1-35.

Luigi, C., Salvatore, D. A., Giovanni, M. and Luigi, R. (2017). Cloud security, Emerging threats and current solutions. Computers and electrical engineering 59, supplement C. (2017): 126-40.

Mazhar, A., Samee, U. K. and Athanasios, V. V. (2015). Security in cloud computing, Opportunities and challenges. *Information Sciences*, 305(2015): 357-83.

Michael, L., Manuel, W. and Helmut, K. (2018). Criteria for selecting cloud service providers, A delphi study of quality-of-service attributes, information & management. Available: https://doi.org/10.1016/j.im.2018.03.004

Minhaj, A. K. (2016). A survey of security issues for cloud computing. *Journal of Network and Computer Applications*, 71: 11-29.

Modi, C., Patel, D., Borisaniya, B., Patel, A. and Rajarajan, M. (2012). A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, 63(2): 561-92.

Muhammad Baqer, M. M., Abul Kalam, A. and Athanasios, V. (2017). Security and privacy challenges in mobile cloud computing, Survey and way ahead. *Journal of Network and Computer Applications*, 84: 38-54.

Munir, K. and Palaniappan, S. (2013). Secure cloud architecture, advanced computing. *An International Journal*, 4(1):

Nabeel, K. and Adil Al-Yasiri (2016). Identifying cloud security threats to strengthen cloud computing adoption framework. *Procedia Computer Science*, 94: 485-90.

Owens, D. (2010). Securing elasticity in the cloud. *Commun ACM*, 53(6): 46-51.

Philipp, S. and Koosha, K. (2017). "Towards continuous security certification of software-as-a-service applications using web application testing techniques. *Advanced Information Networking and Applications (AINA) 2017 IEEE 31st International Conference on*: 931-38.

Ponemon (2011). *Security of cloud computing providers study.* CA Technologies. http://www.ca.com/~/media/Files/IndustryResearch/securityof-cloud-computing-providers-final-april-2011.pdf

Ramachandran, M. (2015). Software security requirements management as an emerging cloud computing service. *International Journal of Information Management*, 36(4): 580-890.

Ramgovind, S., Eloff, M. M. and Smith, E. (2010). The management of security in cloud computing, in the proceeding of information security for South Africa (ISSA). 1-7.

Ravi Kumar, P., Herbert Rajb, P. and Jelcianac, P., 2017. "Exploring data security issues and solutions in cloud computing." In *6th International Conference on Smart Computing and Communications, ICSCC.* pp. 7-8.

Rebecca, A. A., Joseph, K. P. and James Ben, H.-A. (2016). Factors affecting cloud computing adoption in a developing country-Ghana, using extended unified theory of acceptance and use of technology (UTAUT2) model. Available: https://www.scribd.com/document/339785378/IRJET-Factors-Affecting-Cloud-Computing-Adoption-in-a-Developing-Country-Ghana-Using-Extended-Unified-Theory-of-Acceptance-and-Use-Of-Technology

Reuben, J. S. (2007). A survey on virtual machine security. Seminar on network security. Technical report, helsinki university of technology,. Available: http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf

Roundup of Cloud Computing Forecasts and Market Estimates (2015). Available: http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates2015/#56c0b0f0740c

Saurabh, S., Young-Sik, J. and Jong, H. P. (2016). A survey on cloud computing security, Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75(2016): 200-22.

Shaikh, F. B. and Haider, S. (2011). Security threats in cloud computing, 6th International conference on internet technology and secured transaction.

Sharon, I. W., Kumar, C. P. C. and Andrew, J. J. W. (2013). A survey on security threats and vulnerabilities in cloud computing. 4(3): Available: https://www.ijser.org/researchpaper/A-Survey-on-Security-Threats-and-Vulnerabilities-In-Cloud-Computing.pdf

Subashini, S. and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications,* 34(1): 1-11.

Subramanian, N. and Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers and Electrical Engineering,* 71: 28-42.

Suryateja, P. S. Threats and vulnerabilities of cloud computing, A Review. *International Journal of Computer Sciences and Engineering,* 6(3): 297-302.

Wang, C. (2009). Cloud computing checklist, how secure is your cloud? (2009). Forrester research. Available: https://www.forrester.com/report/Cloud+Computing+Checklist+How+Secure+Is+Your+Cloud/-/E-RES55453

Yasir, A. H. and Marwan, D. O. (2013). Cloud computing security, Abuse and nefarious use of cloud computting. *International Journal of Computational Engineering Research*, 3(6): 22-27.

Zhang, S., Zhang, S., Chen, X. and Huo, X., 2010. "Cloud computing research and development trend." *In Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA.* pp. 93-97.