International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

An apprasail on Security of Cloud Computing Environment

Ravi Shanker Singh[1]
Dr.Sayed Hauider Abbas [2]
Phd Researchscholar, Department Of Computer Science ,Sunrise University, Alwar(Raj.)India[1]
Assistant Professor, Department Of Computer Science ,Sunrise University, Alwar(Raj.)India[2]

Abstract

Cloud computing is a new computing paradigm that benefit from the distributed resources to solve large scale computing problems. During the last few years, cloud computing has grown rapidly as promising business idea in the IT industry due to its characteristics such as cost reduction, flexibility, convenience, and scalability. Unfortunately, there are several issues reduce the cloud computing growth such as loss of security, privacy, and control. The security problem is considered a major factor that could prevent the development of cloud computing. In this paper, we explored the cloud computing classification, challenges, and opportunities. Moreover, we review and discuss the cloud computing security issues and accountability. We emphasize that although there are many security models were proposed to improve the cloud security, but there is no any currently available solution to handle all security issues. Therefore, the future research has to be focus on solving the security issues and an accountability mechanism has to be developed. Keywords: Cloud computing, security issues, deployment models, accountability.

1. Introduction

The term of the cloud computing came from the Internet computing or computation via Internet, where many flowcharts and diagrams represent the Internet as a cloud shape. The National Institute of Standards and Technology (NIST) defined the cloud computing as a central storage of computing resources that can accessed on-demands from anywhere through any type of devices with a minimal management effort (Mell and Grance, 2011). Through a NIST definition, the cloud computing includes three service models, four deployment models and five essential characteristics as shown in Figure 1. The three service models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The cloud computing are

categorized as public, private, community, and hybrid based on their deployed service model.

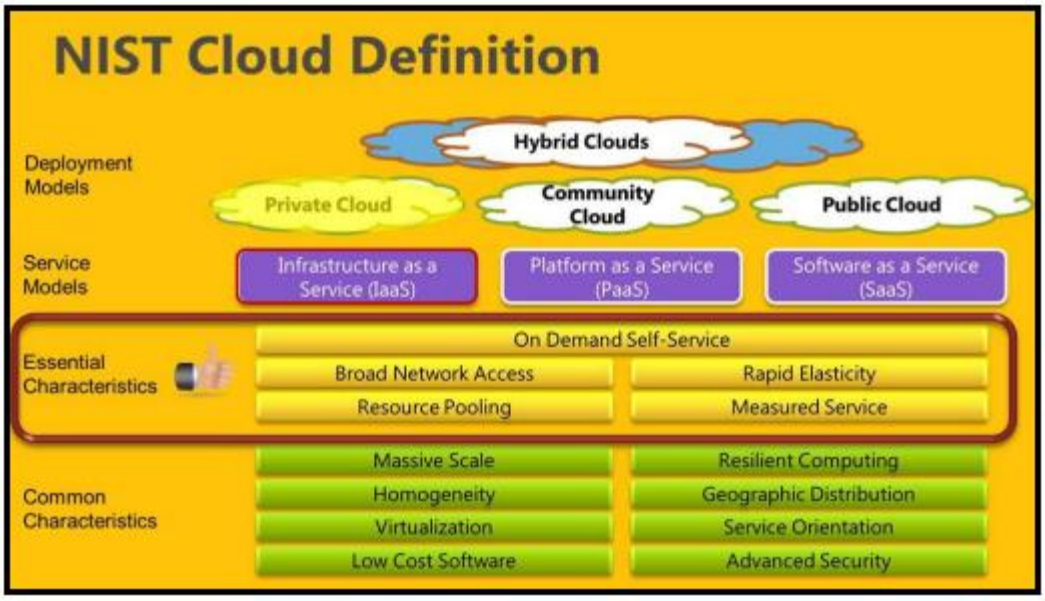

Figure 1: Cloud computing service models, deployment models, and essential and common characteristics (Joyner, 2011)

The power of cloud computing is come from virtualization technology, which creates one or more virtual machine in the host computer by running an application called a hypervisor. These virtual machines simulate the work of physical computer and can run any type of software. Grid computing is considered from one of many technologies that developed cloud computing. Virtualization technology in cloud computing solved many challenges that appeared in grid computing. Grid computing aims to maximize the utilization by reserving multiple servers to perform a single task, while a cloud computing maximizes the utilization by allowing a single server to perform multiple tasks in the same time via a virtualization technology.

The combination of virtualization layer with management layer achieves a highly effective management service. Specifically, the management layer is responsible for monitoring the network traffic and takes a decision to add new servers in rush time or drop server in an idle time Moreover, cloud computing offers economical, flexible, reliable, scalable, and convenient on-demand computing service. Cloud computing can be flexible by offering a service on-demand as much as needed automatically, and scalable by adding or dropping a new server into a network. It can be accessed via broad types of machines such as PDA, Laptop, desktop, and mobile phones.

Unfortunately, cloud computing technology suffers from several problems such as loss of control

and security issues. This problem can affect the adoption and rapid development of cloud computing. Many concerns are considered on the security issue, since the cloud computing service based on transferring data between the service provider and subscriber into two-ways. Consequently, the risk on the data breach is increased. Extensive testing showed that single security method does not provide a secure environment in cloud computing and they suggest to combine more than one method to provide a comprehensive security model.

This paper is organized as follows. First, we will introduce and discuss cloud computing classification. Then, a briefly discussion about cloud computing challenges and opportunities will be presented. Subsequently, we will provide a literature review of cloud computing security. After that, the security issues of cloud computing are explained and discussed in details. Then, we will discuss and focus on the accountability in the cloud. Finally, a discussion and future works are presented and then the conclusion is given.

2. Cloud Computing Classification

Cloud computing is classified into three models based on the type of provided service to the subscriber: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Software as a Service (SaaS) model provides the subscriber with the software application that is he/she needs as a service via a client interface such as a web browser. Therefore, the subscriber doesn't have a control on cloud infrastructure such as, storage, operating system, and network. The service provider hosts the software application so the subscriber does not bother in buying, installing, or managing the software. The subscriber just can connect and use the application with a limited control over application configuration settings. The Platform as a Service (PaaS) model in cloud computing provide a subscriber a platform as a service to deploy their applications on the cloud infrastructure. Herein, the subscriber does not have a control over infrastructure such as a network, operating systems, and storage, but they can control their deployed applications and its hosting environment setting. So, the subscriber can deploy their applications without worrying about the cost of buying any hardware and the inconvenience of resources managing. In addition, the service provider is responsible to provide the subscriber with the pre-installed software that is used in PaaS model. In the Infrastructure as a Service (IaaS), the subscriber can access to the underlying infrastructure and they can also deploy their applications on it. The subscriber has a control over storage, database, deployed

applications, other computing resources, and limited control to some network component.

Based on the NIST definition, the cloud computing is categorized as public, private, community, and hybrid based on their deployed service model. The private cloud is where the cloud computing service is available for a certain organization inside a firewall and is not available for general public. Public cloud provides on-demand cloud computing services for general public via internet that is owned by an organization that provide a cloud services. When several organizations shared same cloud services that support their community concerns, the deployed model is called a community cloud. Some organizations run their private cloud inside the organized and shared a public or community cloud service at the same time. Such deployed model is called hybrid cloud.

3. Cloud Computing: Challenges and Opportunities

In the last few years, cloud computing has been grown very fast and many people and organizations are moving toward placing their services on the cloud. The property of the cloud allows for many concerns to face the growing process. A conducted survey by International Data Corporation (IDC) showed that the security is the major issue that affect the adoption of cloud computing (Gens, 2009), as shown in Figure 2. Since the system architecture of the cloud is different from other traditional system, the traditional security techniques are not enough to provide a secure environment. Therefore, specialized security techniques that meet the requirement of the cloud computing environment are required.

In cloud computing, the deployed service model can be provided on a private or public level. Provide a secure environment in the private cloud is an easy task since the data are bounded within a certain organization within a firewall and it is not available for general public. On the other hand, providing a secure environment in the public cloud is considered a hard and complex task, since the data are available on the internet outside the firewall. In cloud computing, the subscribers cannot control their data by themselves. They do not know the location of the data, the network that transmit the data, and the server that process the data. Thus, they cannot guarantee how much the cloud environment is secure.

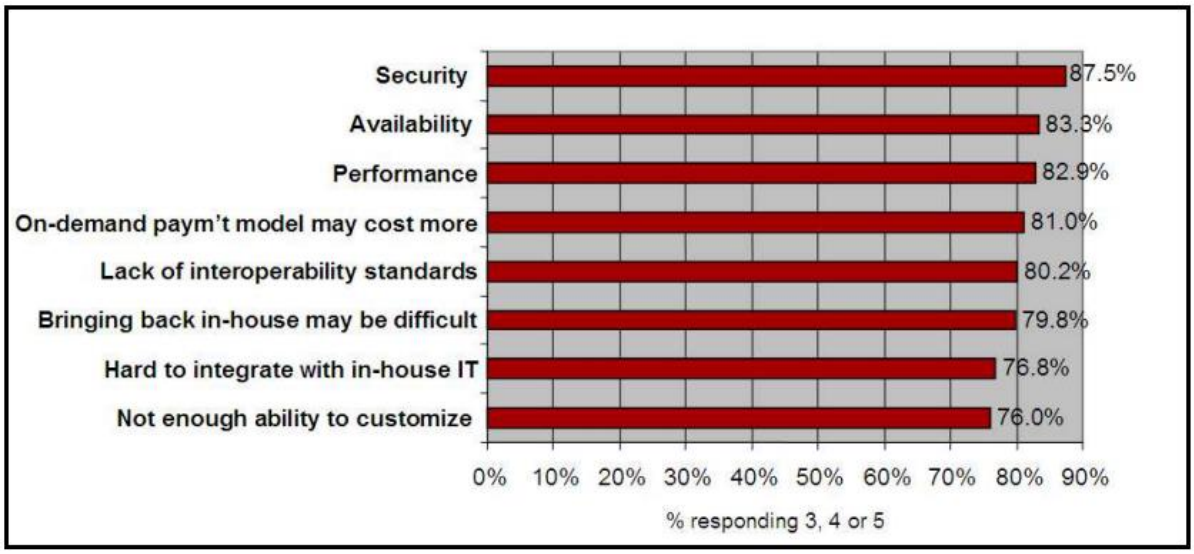

Figure 2: Cloud computing challenges (Gens, 2009)

Security issue has a big concern in cloud computing due to its nature of virtualization, elasticity, scalability, and ubiquity of the data; in which a cloud system needs more security protection from intentionally changes and must be protected to be accessed from unauthorized people. Availability of more data than a service's needs, an extra protection is required for the cloud. In addition, a two-way transmission between service provider and subscriber raises more concerns on the security issue. Most of the time, management of this communication between service provider and the subscriber is controlled by a third-party that increases from the security risk of this system. Therefore, the security issue in cloud computing needs to be studied and solved according to its architecture to provide a high-quality service with a guarantee to protect the data. Extensive testing showed that single security method does not provide a secure environment in cloud computing and they suggest to combine more than one method to provide a comprehensive security model.

4. Literature Review of Cloud Computing Security

Lombardi et al. investigated how a virtualized cloud computing can be more secured by protecting the reliability of virtual machine user and Component of cloud platform (Lombardi and Di Pietro, 2011). They proposed a novel system to increase the security of cloud resources

that is called Advanced Cloud Protection System (ACPS). ACPS can respond locally to any violation in security and send a notification to a security management layer. ACPS prototype is implemented on Eucalyptus and Open ECP open access solutions. They tested the system effectiveness against attacks and the performance under different workloads. The results showed that ACPS was effective in the cloud system protection and the overhead of the generated performance was acceptable when it compared with the provided protection.

Based on data mining techniques, a Hidden Markov Model (HMM) using clustering was proposed to detect any type of security breach in the cloud computing network (Kumar et al., 2011). The administrator can provide a safe cloud environment by using HMM with the help of network filter, which is responsible for monitoring subscriber behaviour continuously and notify the administrator about any event. Clustering analysis was used to decline database searching time. The proposed model can detect any violation easily with a help of HMM even if the intruder will login with a valid username and password. The network was attached with plug-in to handle the subscribers' request efficiently, especially in case of data loss or corruption. Moreover, plug-in helped to be reduced from the cloud environment heavy load when connected to another one of the same types.

Rabai et al., (2013) proposed a quantitative model for a security measurement that permit to the service provider and subscriber in the cloud environment to assess the available risk to their resources, and consequently they can decide according to this security issue. The proposed metric was measured in economic terms that can be determined later according to the available risk. AlZain et al., (2011) proposed a Multi-Clouds Service Model (MCDB) to provide a more secure environment by reducing the security risks and satisfying security requirements. This model based on multiple service providers rather than single service provider of cloud computing that used Shamir's secret sharing algorithm. MCDB model was compared with a single service provider on data integrity, data intrusion, and service availability. The results showed that the security requirements were more satisfied by using multiple-cloud model instead of single-cloud model.

A new collaborative cloud security management framework was proposed by (Almorsy et al., 2011) that was enabling the cloud computing model to satisfy NIST-FISM security certificate to provide a more secure cloud environment. Their framework based on improving the collaboration between three parties: cloud provider, service provider, and subscriber to provide a

more secure cloud platform and hosted service. The framework was build based on a set of security standards to help in automating the security management process. The validity of the framework was proofed by developing a prototype for this framework and employing it in a cloud hosting platform (SaaS application). The framework was evaluated by managing the security of multi-tenant that had the same cloud application. The proposed framework can be exploited to control the security of cloud platform by the cloud provider and the security of hosted cloud service by subscriber.

5. Security Issues

Several researchers consider the IT and its flexibility as an enabler to achieve the desired competitive advantages, considered as a strategic weapon, and as a crucial support to operational and strategic business processes (Masa'deh et al., 2014, Masa'deh et al., 2013b, Masa'deh et al., 2013a, Al Azmi et al., 2012, Masa'deh, 2012, Maqableh, 2012). In cloud computing, two main parties are involved in cloud computing systems: the service provider and the service subscribers as individual or enterprise. Each enterprise has its own sensitive data that need to be very secured and protected from unauthorized access and control (Abdul Nasir Khan et al., 2013). In cloud computing, the enterprise is stored the sensitive data outside of its boundary (provider side). Therefore, the service providers should adopt security system that can prevent unauthorized people from accessing or controlling their data by malicious people from inside and outside the service provider side. This normally can be maintained using several detection, prevention, and encryption techniques. The most important security issues in cloud computing are: trust, integrity, availability, authentication and authorization, and confidentiality (Kshetri, 2013, Almorsy et al., 2011, Lombardi and Di Pietro, 2011, Stinchcombe, 2009, Mansfield-Devine, 2008, Subashini and Kavitha, 2011, Abdul Nasir Khan et al., 2013).

5.1 Trust

Trust refers to the willingness status to depend of one party on another party to achieve a planned goal (Rong et al., 2013). It is a well-known concept in the computer science and being applied in different areas, which is used to show the system users that the system is secure and correct

(Subashini and Kavitha, 2011). The subscriber trust to an organization is known as the ability of an organization to supply the required services to the subscriber's exactly as expected without errors. Trust can be ensured by powerful security policies and constraints on data access by people (Zissis and Lekkas, 2012). In many cases in the cloud, the consumer depends on the providers on storing his/her confidential data on the provider resource (Rabai et al., 2013). Thus, in cloud computing, subscriber and provider should trust each other.

In a cloud environment, trust issue is mainly based on the selected deployment model, as data, processes, and applications control are outsourced (Rong et al., 2013). In public clouds, the control is granted to the subscriber to reduce potential risks by applying the service provider certain security policy and using different applications and tools to increase subscriber trust. In private cloud, data, processes, and applications are owned and managed by the infrastructure's owner. Thus, there is no more security challenges are introduced as trust remains within the organization. Lack of subscriber trust in cloud deployment models can cause several problems. In community cloud, the organizations should trust each other as they are sharing same cloud services that support their community concerns. While, in hybrid cloud the organizations should trust each other and trust the public cloud service provider.

5.2 Availability

Availability refers to the ability of the cloud subscriber to retrieve the needed data at any time (Zissis and Lekkas, 2012, Rabai et al., 2013). One main concern for every enterprise is how they can maintain the access of cloud computing services at any time. A system is called available when an authorized entity can use and access the system and the stored data at any time (Subashini and Kavitha, 2011). Therefore, service provider should ensure that the data available is available to subscriber from different locations at any time. Cloud computing system should keep on working even if there is a security attack. Threats that may face the cloud service availability can be network based attacks such as Distributed Denial of Service (DDoS) attack (Rabai et al., 2013). Moreover, the provider should maintain an appropriate action plan for the emergency and unplanned cases to guarantee the business continuity and disaster recovery to ensure the safety and minimal downtime.

Data can be classified into two main classifications: critical data and archive data. Critical data is

that data needed at any time by subscriber and any delay or unavailability will disrupt him/her. On the other hand, the archival data is that data accessed very seldom and at non-crucial time. Therefore, delay in access to it will not consider as main issue or case, but delaying the critical data is very important issue and could be very costly as the subscriber will not operate normally.

5.3 Integrity

One of the main aspects of information security aspects is the integrity, that refers to assurance that the users' data are not modified without authorization (Rabai et al., 2013, Zissis and Lekkas, 2012). It means that the data, software, and hardware will be modified only by authorized parties or in authorized method (Zissis and Lekkas, 2012). System users need to know that their data is kept out of damage or lost by intentional or unintentional activity (Kshetri, 2013). In cloud computing, data integrity is considered as a major factor to success the cloud computing as it will increase the subscriber trust and satisfaction that maintained by the provider and the subscriber (Abdul Nasir Khan et al., 2013). Maintaining the integrity of cloud computing is considered as a main challenge to cloud parties, as the threats could be at the subscribers or providers sides. To ensure data integrity in the provider and subscriber sides, a secure encryption algorithm could be used, but it could not guarantee that data did not change through locating it in the cloud (Subashini and Kavitha, 2011). Violating the integrity of critical data in the cloud could be very costly as the subscriber will not be able to operate normally. Moreover, cloud provider should consider data recovery plan in case that any disaster event might happen.

5.4 Authentication and Authorization

Authentication refers to the process that is used proves the users claimed identity while they are trying to access any system (Rabai et al., 2013, Turban and King, 2012, Subashini and Kavitha, 2011). It is the user's ability to verify their accounts through suitable standard and available mechanisms by establishing confidence in user identities, while they are being presented to an information system (Zissis and Lekkas, 2012). However, authorization is to grant the users a permission to do what they are trying to do. Authorization is the process that used to identify the

functions and the actions that the user is allowed to perform. Lack of strong authentication may cause unauthorized access to users account on a cloud, which may lead to privacy violation. Lack of authorization in cloud computing leads to privacy breach as the users account will be accessed by unauthorized parties. Also, if a cloud user uploaded a file to share it with other users, then there should be a mechanism to confirm the creator of the file, which can be achieved by applying the authentication mechanism.

5.5 Confidentiality

Cloud computing is based on sharing the same resources by multiple users at different levels (Network, Host, and Application) (Avram, 2014, Zissis and Lekkas, 2012). Increasing number of involved parties in cloud computing will increase the risks. Confidentiality refers to data privacy and accuracy by protecting private and sensitive data (Turban and King, 2012).

In cloud environment, confidentiality is one of the main used aspects to ensure the control the data of an organization across multiple distributed databases. The subscriber private and sensitive data need to be protected from being disclosed to unauthorized individual, organizations, or any other entities. The subscriber data can be classified into different categories based on its importance (Zissis and Lekkas, 2012, Abdul Nasir Khan et al., 2013). Thus, fail to protect the subscriber data from unauthorized access can cause series of problems that could be very costly. Confidentiality can be guaranteed using encryption techniques with respect to symmetric or asymmetric encryption algorithms. Could subscribers can ensure the data confidentiality on their sides by encrypting it before uploading. In cloud environment, data confidentiality is related to user authentication by protecting their accounts from theft (Subashini and Kavitha, 2011). Thus, lack of strong authentication mechanism may lead to privacy violation. The cloud provider should provide secure cloud environment to ensure users privacy. Privacy refers to users' right to control disclosure of their personal data (Kshetri, 2013). Cloud subscribers needs to guarantee that their personal data is protected appropriately. In cloud, subscriber data are stored in data center that have potential risks. Therefore, cloud provider should implement different security techniques to assure data privacy. Encryption algorithms can be used to protect subscriber data against malicious attacks. Wherever you find security dimensions then you find availability, confidentiality, and integrity combined with each other

because one leads to another (Maqableh et al., 2008, Maqableh, 2010b, Maqableh and Dantchev, 2009, Maqableh, 2010a, Maqableh, 2011, Maqableh, 2012).

6. Accountability in the Cloud

In cloud computing system, the behaviour of service provider and subscriber is determined on a predefined Service Level Agreement (SLA) (Rong et al., 2013). The validity of this system is determined by the correctness of the SLA, and to what extend the subscriber complies with it. Any breach into this agreement is considered as a violation. Therefore, a robust technique to detect this violation is required in order to build a trusted computing environment. However, the complicated nature of service provision chains in cloud computing makes detecting and preventing the violation a significant challenge.

Accountability is one of the mechanisms that are used to provide a trustworthy computing environment by improving the data protection at different levels (October 2009). Accountability is defined as a commitment of the organization for accepting actor of the host for the personal data that are entrusted in the computing environment from the collection time until when it is destroyed. This commitment also involves presenting a proper remedy to any failure. The notion of accountability has been established by the Organization for Economic Cooperation and Development (OECD). Pearson (Siani, 2011) declares that the main components of the accountability are: Responsibility, Transparency, Assurance, and Remediation. She also discussed that the accountability should be retrospective and prospective by extending the security rules to prevent the fault from happening and takes an action if happen.

Consequently, some researchers in this field successfully implement the accountability in their systems. A novel approach to provide a Service Oriented Architecture (SOA) by enforcing a strong accountability in cloud computing is proposed by Yao et al (Yao J et al., 2000). In this system, the accountability is enforced on the service provider and the fault is always identified by their causer with supported evidence. Another study is conducted by Pearson (Pearson Siani and Andrew., 2009) to illustrate how the accountability as a path forward can resolve the privacy and security threats within the cloud.

7. Discussion and Future Works

Cloud computing one of the recent emerge modern technology and one of the active research areas that has a promising future. Cloud computing users can access cloud services at anytime and anywhere. It has business benefits and at the same time potential risks. Cloud security issues research is related to different areas that can play major role to solve the security problems. The culture, ethical, legal, and political factors have extremely important role in this area. Cloud providers offer services through cloud system and resources. Therefore, cloud environment has potential risks similar to any other Internet-based systems. Cloud is considered as an interested and important that introduced in the IT industry. Thus, IT industry needs to move to cloud computing, which requires to consider several important issues such as security. Also, enterprises need to implement cloud computing to help them in reducing the cost and increase the efficiency.

Many enterprises are worried about cloud security issues, which prevent them from using cloud services. At the same time, other enterprises that use the cloud service for less sensitive and unimportant data and use their local network to keep the sensitive and important data. The cloud providers are encountering major pressures and challenges in protecting subscribers' private and sensitive data and information assets. There are several issues in cloud need to be considered in the future research such as security, privacy, performance, accountability, ownership, performance, and other non-technical issues. Therefore, researchers are facing many challenges and need to find solutions for the technical and non-technical issues. The security issues need to be investigated deeply.

8. Conclusions

In this paper, we presented an overview of cloud computing concepts, characteristics, challenges, and opportunities. A survey related to cloud security issues was presented. We also reviewed and discussed the cloud computing security issues and accountability. Moreover, we highlighted the trust, availability, integrity, authentication and authorization, and confidentiality issues relevant to cloud computing.

Cloud computing has very promising characteristics such flexibility, reliability, scalability, and

cost reduction. Cloud security issues are considered as main challenge for the cloud users and providers. The subscribers' mistrust of cloud security and privacy limit the number of cloud subscribers. They prefer to use the company or private systems rather than cloud system, as they fell much more confident about the security and privacy issues. Therefore, cloud providers should provide high protection measurable mechanisms for cloud subscribers to be more confident about the privacy and security issues.

Nowadays, cloud computing cannot replace completely the traditional computing due to some problem in different deployment models as several large enterprises and government do not accept it fully. Therefore, new cloud security solutions are required to increase subscribers and providers security and privacy concerns. Several security issues in cloud need to be investigated deeply to strength the cloud security capability. Solving the current cloud problems will encourage increasing its adoption rate.

References

(October 2009) Centre for Information Policy Leadership (CIPL). Data Protection Accountability: The Essential Elements.

- ABDUL NASIR KHAN, M.L. MAT KIAH, SAMEE U. KHAN & MADANI, S. A. (2013) Towards secure mobile cloud computing: A survey. Future Generation Computer Systems, 29, 1278- 1299.
- AL AZMI, N., AL-LOZI, M., AL-ZU'BI, Z., DAHIYAT, S. & MASA'DEH, R. (2012) Patients Attitudes toward Service Quality and its Impact on their Satisfaction in Physical Therapy in KSA Hospitals. The European Journal of Social Sciences, 34, 300-314.
- ALMORSY, M., GRUNDY, J. & IBRAHIM, A. S. (2011) Collaboration-Based Cloud Computing Security Management Framework. IEEE 4th International Conference on Cloud Computing.
- ALZAIN, M. A., SOH, B. & PARDEDE, E. (2011) MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing. Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing.
- AVRAM, M. G. (2014) Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. Procedia Technology, 12, 529-534.
- GENS, F. (2009) New IDC It Cloud Services Survey: Top Benefits and Challenges.

- JOYNER, J. (2011) How cloudy is your cloud? The NIST offers a cloud standard. [Online], [Retrieved May 01, 2014], teacher public, http://www.techrepublic.com/blog/data-center/how-cloudy-is-your-cloud-the-nist-offers-a-cloud-standard/4635/.
- KSHETRI, N. (2013) Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37, 372-386.
- KUMAR, P., NITIN, N., SEHGAL, V., SHAH, K., SHUKLA, S. S. P. & CHAUHAN, D. S. (2011) A Novel Approach for Security in Cloud Computing using Hidden Markov Model and Clustering. 2011 World Congress on Information and Communication Technologies (WICT).
- LOMBARDI, F. & DI PIETRO, R. (2011) Secure virtualization for cloud computing. Journal of Network and Computer Applications, 34, 1113-1122.
- MANSFIELD-DEVINE, S. (2008) Danger in the clouds. Network Security, 2008, 9-11.
- MAQABLEH, M., SAMSUDIN, A. & ALIA, M. (2008) New Hash Function Based on Chaos Theory (CHA-1).
- MAQABLEH, M. M. (2010a) Fast Hash Function Based on BCCM Encryption Algorithm for E-Commerce (HFBCCM). 5th International Conference on e-Commerce in Developing Countries: with focus on export. Kish Island - Iran., IEEE.
- MAQABLEH, M. M. (2010b) Secure Hash Functions Based On Chaotic Maps For E-Commerce Applications. International Journal of Information Technology and Management Information Systems (IJITMIS).
- MAQABLEH, M. M. (2011) Fast Parallel Keyed Hash Functions Based on Chaotic Maps (PKHC). Western European Workshop on Research in Cryptology. Weimar - Germany. Lecture Notes in Computer Science.
- MAQABLEH, M. M. (2012) Analysis and Design Security Primitives Based on Chaotic Systems for eCommerce. Durham University.
- MAQABLEH, M. M. & DANTCHEV, S. (2009) Cryptanalysis of Chaos-based Hash Function (CBHF). First International Alternative Workshop on Aggressive Computing and Security (iAWACS). Laval - France., iAWACS.
- MASA'DEH, R. M. T., MAQABLEH, M. M. & KARAJEH, H. (2014) A Theoretical Perspective on the Relationship between Leadership Development, Knowledge Management Capability, and Firm Performance.
- MASA'DEH, R. (2012) The Impact of Management Information Systems (MIS) on Quality Assurance (QA): A Case Study in Jordan. the International Journal of Information, Business and Management, 4, 93-110.

- MASA'DEH, R., GHARAIBEH, A., MAQABLEH, M. & KARAJEH, H. (2013a) An Empirical Study of Antecedents and Outcomes of Knowledge Sharing Capability in Jordanian Telecommunication Firms: A Structural Equation Modelling Approach. the Life Science Journal, 10, 2284 -2296.
- MASA'DEH, R., SHANNAK, R. & MAQABLEH, M. (2013b) A Structural Equation Modelling Approach for Determining Antecedents and Outcomes of Students' Attitude toward Mobile Commerce Adoption. the Life Science Journal, 10, 2321-2333.
- MELL, P. & GRANCE, T. (September 2011) The NIST definition of cloud computing. National Institute of Standards and Technology - Special Publication 800-145.
- PEARSON SIANI & ANDREW., C. (2009) Accountability as a way forward for privacy protection in the cloud.
- IN JAATUN, M. G., ZHAO, G. & RONG, C. (Eds.) Cloud Computing. Springer Berlin Heidelberg.
- RABAI, L. B. A., JOUINI, M., AISSA, A. B. & MILI, A. (2013) A cybersecurity model in cloud computing environments. Journal of King Saud University - Computer and Information Sciences, 25, 63-75.
- RONG, C., NGUYEN, S. T. & JAATUN, M. G. (2013) Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39, 47-54.
- SIANI, P. (2011) Toward accountability in the cloud. IEEE Internet Computing, 15, 64 - 69.
- STINCHCOMBE, N. (2009) Cloud computing in the spotlight. Info security, 6, 30-33.
- SUBASHINI, S. & KAVITHA, V. (2011) A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34, 1-11.
- TURBAN, E. & KING, D. (2012) Electronic commerce 2012 global edition, person.
- YAO J, CHEN S, WANG C, LEVY D & J., Z. (2000) Accountability as a Service for the Cloud. Proc. 6th IEEE World Congress on Services.
- ZISSIS, D. & LEKKAS, D. (2012) Addressing cloud computing security issues. Future Generation Computer Systems, 28, 583-592