STRATEGIES FOR CLOUD COMPUTING ADOPTION

Solution Suggestions Regarding the Use of Cloud Computing in the Public Organizations

Alssull I. M. M.[1] and Kerwad Z. A. M.[2]
[1]Internet Systems Department, Information Technology Faculty, Misurata University
[2]Information Systems Department, Information Technology Faculty, Misurata University

submittion date: 21-06-2021 acceptance date: 28-06-2021 publishing date: 01-10-2021

Abstract:
The development in information systems, which took place on a certain scale in the second half of the 20th century, gained momentum in the first quarter of the 21st century; The rapid increase in the intensity and diversity of user demands, together with the technological innovations and changes in software and hardware components, made it necessary to use new methodologies in information architectures. Virtualization, service-oriented architecture, server-client model, distributed computing, etc. cloud computing, a service model that emerged with the development and integration of pioneering technologies and concepts; It offers low-cost, flexible, scalable, platform-independent accessible and high-performance architectures to its users.This paper aims to exmine the strategies for cloud computing adoption through solution suggestions regarding the use of cloud computing in the public organizations.

Keywords: Strategies, Cloud Computing, Public Organizations, Solution, Suggestions.

Introduction

Cloud computing is a new term in the computing world [1] and it signals the advent of a new computing paradigm [1,2]. Computing emerged in the early 1990s, as high performance computers were inter-connected via fast data communication links, with the aim of supporting complex calculations and dataintensive scientific applications. Grid computing is defined as a hardware and software infrastructure that provides dependable consistent, pervasive, and inexpensive access to high-end computational capabilities. Cloud Computing has resulted from the convergence of grid computing, utility computing and SaaS, and essentially represents the increasing trend towards the external deployment of IT resources, such as computational power, storage or business applications, and obtaining them as services [3].

Throughout computer science history, numerous attempts have been made to disengage users from computer hardware needs, from time-sharing utilities envisioned in the 1960s, network computers of the 1990s, to the commercial grid systems of more recent years [4].

This new paradigm is quickly developing and attracts a number of customers and vendors alike. The quick development of cloud computing is being fuelled by the emerging computing technologies which allows for reasonably priced use of

computing infrastructures and mass storage capabilities [5]. It also removes the need for heavy upfront investment in Information Technology (IT) infrastructure.

This is steadily becoming a reality as a number of academic and business leaders in this field of science are spiralling towards cloud computing. Cloud computing is an innovative Information System (IS) architecture, visualized as what may be the future of computing, a driving force demanding from its audience to rethink their understanding of operating systems, client–server architectures, and browsers. Cloud computing has leveraged users from hardware requirements, while reducing overall client side requirements and complexity [6].

The name cloud computing, was inspired by the cloud symbol that is often used to represent the Internet in flow charts and diagrams. A distinct migration to the clouds has been taking place over recent years with end users, ‘‘bit by bit’’ maintaining a growing number of personal data, including bookmarks, photographs, music files and much more, on remote servers accessible via a network [7]. Cloud computing is empowered by virtualization technology; a technology that actually dates back to 1967, but for decades was available only on mainframe systems. In its quintessence, a host computer runs an application known as a hypervisor; this creates one or more virtual machines, which simulate physical computers so faithfully, that the simulations can run any software, from operating systems, to end-user applications[7,8] .

Cloud computing is a computing paradigm that involves outsourcing of computing resources with the capabilities of expendable resource scalability, on demand provisioning with little or no up-front IT infrastructure investment costs. [9,10] Cloud computing offers its benefits through three types of service or delivery models namely infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-Service (SaaS). It also delivers its service through four deployment models namely, public cloud, private cloud, community cloud and hybrid cloud [10]. Cloud computing is viewed as one of the most promising technologies in computing today, inherently able to address a number of issues.

A number of key characteristics of cloud computing have been identified [11]. Flexibility, users can rapidly provision computing resources, as needed, without human interaction. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out or up. Scalability of infrastructure: new nodes can be added or dropped from the network as can physical servers, with limited modifications to infrastructure set up and software.

Cloud architecture can scale horizontally or vertically, according to demand. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous platforms (e.g., mobile phones, laptops, and PDAs) [12]. There is a sense of location independence, in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Reliability improves through the use of multiple redundant sites, which makes cloud computing suitable for business continuity and disaster recovery. Economies of scale and cost effectiveness.

Cloud implementations, regardless of the deployment model, tend to be as large as possible in order to take advantage of economies of scale[13,14,15]. Large cloud

deployments can often be located close to cheap power stations and in low-priced real estate, to lower costs. Sustainability comes about through improved resource utilization, more efficient systems, and carbon neutrality.
Cloud implementations often contain advanced security technologies, mostly available due to the centralization of data and universal architecture [16]. The homogeneous resource pooled nature of the cloud, enables cloud providers, to focus all their security resources on securing the cloud architecture. At the same time, the automation capabilities within a cloud, combined with the large focused security resources, usually result in advanced security capabilities.

Literature Review

Barriers to Cloud Computing Adoption in the Enterprise
Although there are many benefits to adopting cloud computing, there are also some significant barriers to adoption [17,18].

Security and privacy because cloud computing represents a new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved. That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing. The ability of cloud computing to adequately address privacy regulations has been called into question. [14]

Connectivity and Open Access The full potential of cloud computing depends on the availability of high-speed access to all. Such connectivity, rather like electricity availability, globally opens the possibility for industry and a new range of consumer products. Connectivity and open access to computing power and information availability through the cloud promotes another era of industrialization and the need for more sophisticated consumer products.

Reliability Enterprise applications are now so critical that they must be reliable and available to support operations. In the event of failure or outages, contingency plans must take effect smoothly, and for disastrous or catastrophic failure, recovery plans must begin with minimum disruption. Additional costs may be associated with the required levels of reliability; however, the business can do only so much to mitigate risks and the cost of a failure. Establishing a track record of reliability will be a prerequisite for widespread adoption.

Interoperability The interoperability and portability of information between private clouds and public clouds are critical enablers for broad adoption of cloud computing by the enterprise. Many companies have made considerable progress toward standardizing their processes, data, and systems through implementation of ERPs.

Economic Value The growth of cloud computing is predicated on the return on investment that accrues. It seems intuitive that by sharing resources to smooth out peaks, paying only for what is used, and cutting upfront capital investment in

deploying IT solutions, the economic value will be there. There will be a need to carefully balance all costs and benefits associated with cloud computing-in both the short and long terms. Hidden costs could include support, disaster recovery, application modification, and data loss insurance.

Changes in the IT Organization The IT organization will be affected by cloud computing, as has been the case with other technology shifts. There are two dimensions to shifts in technology. The first is acquiring the new skill sets to deploy the technology in the context of solving a business problem, and the second is how the technology changes the IT role. During the COBOL era, users rarely programmed, the expectations of the user interface varied, and the adaptability of the solution was low.
Even though, political issues due to global boundaries in the cloud computing world, there is variability in terms of where the physical data resides, where processing takes place, and from where the data is accessed. Given this variability, different privacy rules and regulations may apply. Because of these varying rules and regulations, by definition politics becomes an element in the adoption of cloud computing, which is effectively multijurisdictional.

Trust and Challenges in cloud computing adoption

Cloud computing has been reported to provide several advantages to businesses and customers that have switched to cloud based services, such as reliability, accessibility, cost reductions, the ability to scale services easily, flexibility, and the reduction of failure rates [19]. However, there are a number of concerns associated with cloud computing [20]. One of the most important challenges is related to security issues [21]. Recent studies have revealed that privacy, security, and trust issues arise as a result of handling computing resources by third parties that can be accessed via a network [22].
In this proposal, security and trust will be investigated further in an attempt to develop a trust model that can be used by clients when choosing a service provider. Security is regarded by many as a make or break concern. Security in cloud computing relates to things other than authenticity, authorization, and responsibility; it also relates to data protection, disaster recovery, and business continuity [23]. The very nature of cloud computing makes security perspectives quite more complex as cloud computing is concerned with relinquishing direct control over numerous aspects of security and privacy [24]. As a result, many Organizations are hesitant to host their internal data on computers that are external to theirs and that might be co-hosted with applications of other companies. Cloud computing adoption is faced with a number of challenges, these challenges are: security challenges, legal and compliance challenges and organisational challenges [25,20]. Linked to all these challenges is the issue of trust between clients and vendors, because cloud computing calls for organisations to trust vendors with the management of their IT resources and data. Trust being a critical factor in cloud computing adoption, this proposal will focus specifically in identifying the challenges facing organisations when seeking to adopt cloud computing. Of all the challenges security has received more mention.

Furthermore, service providers have access to all the data and could deliberately or accidentally use it for unapproved purposes [26,29] by doing so organizations are conferring a high level of trust into the cloud provider [27,28]. Trust is perceived as a key concern for end-user consumers, organizational customers, and regulators. Lack of trust is a major inhibitor to the adoption of cloud services, as people are suspicious about what happens to their data once it goes into the cloud [30,31].

Research Methodology

The recommendations and solution proposals of the European Union Network and Information Security Agency (ENISA) for the establishment of secure public clouds according to the current situation in Europe and the foreseen scenarios regarding the adoption of cloud computing in European countries are as follows:

- Member States (MS) and the European Commission (EC) support the development of the EU strategy to ensure the adoption of public clouds,
- The European Commission (EC) and Member States (MS) develop a business model to ensure the sustainability and affordability of public cloud solutions,
- Member States (MS) and cloud providers encourage the development of a framework to mitigate the "loss of control" problem,
- The European Commission (EC) and Member States (MS) encourage the definition of a regulatory framework to solve the "locality problem",
- Member States (MS) and cloud providers encourage the development of public cloud solutions that comply with EU and country-specific regulations,
- A Service Level of the European Commission (EC) and Member States (MS)
- Support the development of the Agreement (SLA) framework,
- The European Commission (EC) and Member States (MS) encourage the adoption of basic security measures for public and private cloud deployment models,
- The European Commission (EC) and Member States (MS) develop a certification framework,
- Encourage academics and cloud providers to research on public cloud security.
- The European Commission (EC) and Member States (MS) support the increase in data privacy in the cloud

RESULTS AND DISCUSSION

The explanations of these suggestions and the precautions to be taken are given below:

Proposition 1: EU public cloud strategy

Cloud computing adoption in the public sector is very heterogeneous in Europe. This slow adoption process; It depends on many reasons such as security, control, data protection and ignorance. Although current or proposed security legislation covers some of the information security requirements, being aware of how IT services will

operate and knowing what security measure revisions cloud adoption will result in has a significant impact on cloud computing use. Studies suggest that systematic adoption of the public cloud is more advanced in countries that have a national strategy to address cloud computing adoption. Moreover, many experts are convinced that the development of an EU strategy that focuses solely on national strategies for public sector and public cloud computing will promote the adoption of public cloud.

Measures:

1. Designing a detailed strategy on high-level principles covering technical, legal and corporate issues.
2. Massive provision of secure cloud services; consider a step-by-step business plan, a program that plans by identifying meaningful outputs and milestones.
3. Encourage cloud deployment and encourage organizations; promoting the use of knowledge-based, risk-based policies and external public cloud solutions for "open data" in the public sector.
4. Linking the national cloud strategy with projects and initiatives to increase the efficiency of information and communication technologies and data center aggregation in the public sector.
5. Evaluate public cloud architecture options (open, private, community, and hybrid) based on the type of services and their requirements, such as privacy, security, and control.
6. Member States' (MS) strategies; the national strategy to ensure that it complies with laws, regulations and national agency requirements on security and data protection, as well as taking into account the confidentiality of data; security, protection of information, assets and infrastructures, etc. ensuring that it complies with national and EU laws and regulations,
7. To develop public service catalogs; evaluate catalogs of cloud products, applications, and services, as well as options that categorize targeted public cloud platforms, usage profiles, and best practices.

Proposition 2: A business model that guarantees sustainability

Today, private cloud architecture is most commonly used in EU public clouds. The low utilization of public cloud architecture is due to the regulatory weaknesses and immaturity of public cloud solutions. There are three major challenges posed by the relative immaturity of the public cloud computing market:

1. Although there are many cloud computing service providers in the market, most of them are at the entry level and therefore cannot guarantee the level of stability that a company capable of collaborating with the public should have,
2. Many solutions are designed in a specific business context and therefore many public cloud solutions on the market cannot meet the specific needs of the public.
3. There are only a few solutions on the market today that can take into account the private responsibility of the public for data protection,

As a result, there are still relatively few public cloud computing solutions on the market that are suitable for use by a government. However, a private cloud can be

expensive to build, operate and transfer existing services to. Developing a cost model capable of real cost savings is difficult.

To increase the adoption of public cloud, the European Commission and Member States' competent authorities, in collaboration with cloud providers, need to develop a business model that will guarantee efficiency and economies of scale of public cloud solutions. The solution is to move towards using an appropriate, open/community cloud architecture. This model will reduce investment costs to increase data and service availability, service reliability and security.

Measures: A regulatory framework is needed to ensure the adoption of multi-tenant infrastructure and service sharing between Member States. This framework should address the issue of data and service locality. The framework should also address issues that come with cloud provider switching or cloud service termination. Here, the terms and conditions that should be in a Service Level Agreement and the applicability of these terms and conditions should be emphasized. Secondly, an independent third-party assurance could contribute to building trust between the provider and customers, so that European SMEs and other organizations will make greater use of cloud computing services. The main idea is to establish a framework within which government agencies can accredit cloud vendors and provide some form of active and efficient escrow service by a third party. In this way, the other party can take over the cloud operations without interruption and cloud provider A can apply to provider B for a user. This software should contain the current status of users' data and transactions. Third, public cloud providers need to increase their reputation and credibility. More specifically, an open/community cloud architecture should support:

- An EU regulation on the use of multi-tenant infrastructures for e-Government services,
- A framework to certify/assess the competence of the public cloud provider (for example, a voluntary certification program that provides transparent audit procedures),
- Public procurement framework for all government bodies that need to provide cloud services,
- A legal framework for dealing with overseas sourcing issues,
- Description of standard procedures for application and data migration,
- A framework for controlling/monitoring data locality and handling data in general.

Proposition 3: A framework to reduce loss of control

Loss of data and resource control stands out as one of the most important obstacles to the public cloud. The "loss of control" problem is not just a matter of technology; it is also a matter of awareness, transparency, regulation, contracts between providers and public customers. For example, when a government agency transfers its owned data and applications to the cloud, it may be concerned about the possibility of the cloud provider accessing and manipulating its data, due to the lack of transparency in the cloud provider's procedures (for example, standard procedures for data corruption), the absence of common contractual provisions and an EU regulation. Another aspect of loss of control is the issue of dependency on

the provider. For example, in the event of provider bankruptcy, concerns may arise about the fate of data and applications. It should always be possible to transfer data and applications from one provider to another cloud provider, without the cost and time constraints of provider dependency. All these provisions need to be declared and understood in the service level agreement.

Measures: European Commission and Member States' competent authorities in cooperation with cloud providers and public customers; they should work to reduce "loss of control" by closely addressing management, monitoring and control, provider dependency and data processing. The steps to be taken in this regard are:

1. Definition of a monitoring and auditing framework for public service tiers in the government cloud.
2. Description of standard procedures for data processing,
3. Definition of standard procedures for data and service transfer,

Proposition 4: A regulatory framework to solve the problem of locality

Cloud providers usually store data in their own data centers, which can be located in many different countries. The possibility of having data and resources outside the country is often perceived as a barrier to public cloud adoption due to data privacy issues. The definition of the regulatory framework for the location of data may reduce public users' objections to cloud architecture, but the most critical concern for data protection is the security of data rather than its location. To achieve this, technical solutions (eg using encryption) are indicated to be suitable. However, the risk is not just about taking technical measures. Usually, local jurisdictions only prohibit the possession of publicly owned data abroad. Secondly, it's not just about the data location, it's also about what legal framework the cloud provider falls within.

It should also be noted that for smaller countries, hosting data abroad has prohibitive costs and it will also be difficult to set up their own data and backup centers. The regulatory framework should take this into account and offer solutions to overcome it.

Measures: For the definition of a new framework, the European Commission and the competent authorities of the Member States, in cooperation with cloud providers and public customers, should work on:

1. Description of the measures necessary to increase the awareness of public institutions and cloud service providers about the current EU legislation on the subject,
2. Encouraging the development of technological solutions in line with the current legislation,
3. Evaluating and classifying public institution requirements regarding data ownership and data privacy according to the type of data available,
4. Improve existing EU legislation on data and resource ownership, with a focus on outsourcing.
5. Improve existing EU legislation on data privacy with a focus on outsourcing.

Proposition 5: Public cloud solutions that comply with EU and national law

Measures should be taken to encourage the development of systems and services that comply with EU regulations and country-specific legislation, in order to allay public authorities' doubts about the technological solutions offered by service providers.

Measures: European Commission and Member States' competent authorities, public bodies, standardization bodies and the R&D sector in cooperation with cloud providers; It should try to encourage the development of technological solutions in line with EU and national legislation. The steps to be taken will be:

1. Establishing an accreditation framework (certification) that certifies or guarantees that each cloud solution complies with relevant legislation (national and/or EU law),
2. Promoting the definition of standard contracts to cover legal compliances,
3. Increasing the awareness of the EU and Member States on regulations,
4. Promoting education on cloud issues for EU states.

Proposition 6: A common framework for the Service Level Agreement (SLA)

The development of a common framework for standard service level agreements will be a measure to increase the deployment of public clouds. By having a service level agreement framework; The challenges that government organizations face, such as the definition of contracts and doubts about public cloud solutions, can be tackled. This work was initiated in the EU Cloud Strategy and is supported by ENISA.

Measures:

1. Assurances and warranties given by cloud providers to government entities; should include specific penetration testing to support security and privacy claims, and should also be verified and evaluated by audit activities by independent third parties. Clients can benefit from validation/comments by third party auditors to avoid duplication of audit.
2. It should be ensured that the obligation to respond and report to the incident is fulfilled and that the providers respond immediately to the incidents. The terms of the contract, which aim to report incidents that appear critical and that may affect the availability of services, to relevant authorities and/or public users, and to recover quickly from attacks and errors, should be implemented.
3. Incident response and reporting is especially necessary for public services that have some level of criticality in terms of service type or data sensitivity. In these cases, it is helpful to separate service level agreements in terms of response and reporting timelines.
4. Penalties for breach of service level restrictions should be included in the contract. In this regard, it seems noteworthy that a similar service contract or a reputation (notation) system should be established to inform users about past violations against similar standardized classifications.

Proposition 7: Security measures for the public cloud

Defining standard approaches and methods for security certification of services and providers is important for reliable use of cloud architectures. In order to ensure the security of public institutions, it is necessary to develop a model that consists of the sophistication levels that cloud providers must comply with through certification

and that clearly defines the requirements at each security level. The accreditation model of cloud services can only be implemented by a dedicated central administration. Public users and providers should be free to choose the level of security demanded and provided for public services, and the relevant departments should be left with the option to implement the best among the most effective and inexpensive financial solutions. A specific set of security measures focused on public cloud deployment will be a way to increase reliability in the cloud supply chain.
Measures: Recommended actions to increase security and information protection in public cloud services:

1. To support the pre-evaluation process before purchasing the service,
2. Establishing a set of basic security measures focused on public clouds (These measures should include areas such as security management, identity management, data backup services and availability, etc.),
3. Including risk impact levels in each area to present a sophisticated/advanced model; enable the audit (and/or certification) framework of information security measures;
4. To promote security labeling systems.

Proposition 8: Certification framework

Considering the public administration framework, it becomes clear that the problem is that certificates are not widespread in public institutions. Government agencies prefer to comply with standards without needing to be approved by an external auditor. Currently, as part of the EU Cloud Strategy, the European Commission has launched activities supporting certifications in the cloud and more importantly is creating a meta-framework for all providers to be accredited. ENISA is part of the industry group chosen to be responsible for this action and fully supports the European Commission. This work was initiated in the EU Cloud Strategy and is supported by ENISA.
Measures:

1. An approach to certification of public cloud platform and services is a controversial and difficult process. The main driver to achieve the goal may be to incorporate this obligation into the EU regulatory framework or a European voluntary certification scheme.
2. Global development and industry-driven standards, as well as public requirements in other countries, must be explored.
3. It is necessary to support the creation of a national "service catalogs of pre-tried cloud products/applications". This approach reduces the cost of the service by applying the "Make sure once, install many times" model.
4. This action can be combined with previous safeguards recommendations, creating a European accreditation system for all providers wishing to offer cloud services to the public sector. In the field of information security, a meta-framework that includes per-domain security controls and is classified into levels of sophistication is a good starting point.

Proposition 9: Promote research on public cloud security

It is important to promote public cloud research by leveraging existing research programs to support the development of cloud technologies aligned with government requirements. Research should be directed towards raising the risk impact level of cloud solutions for utilities.

With the cooperation of the European Commission and the R&D authorities of the Member States and academic; cloud providers should support existing and future national and European research programs and incorporate their own work on security aspects of cloud computing in the public sector into their research programmes. Some of these research topics are: Cloud service lifecycle management, cloud supply chain control, event management, cyber risk analysis, cyber threat modeling, encryption, data protection, cloud privacy and security measurement, privacy level agreement, accountability and transparency for data protection and information security in cloud systems.

Measures: European Commission and competent authorities of Member States; cloud providers should undertake the following actions with government customers, the R&D industry and academic collaboration:

1. Establishing priorities for different research objectives,
2. Communicating with existing security research programs at EU and national level (such as Horizon 2020),
3. Working with appropriate institutions and organizations (eg Framework Program Committee and Advisory Groups, Technology Platforms, etc.) to define an appropriate program of study.

Proposition 10: Enforcement of data privacy

Data protection is an important issue due to the sensitivity of information processed within public clouds. The cloud services of the European Commission and Member States need to be ensured to comply with EU data protection laws. To guarantee privacy in cloud services, encryption by cloud provider and authenticated access by users seems like a simple solution. However, the implementation of cryptographic solutions in cloud services is still at a low level of development.

Measures: Data protection enforcement techniques have become a fundamental issue and controlled and cryptographic techniques such as:

1. Up-to-date policies on the management of personal information by the organization, which are clearly expressed and include information obtained with possible footnotes from foreign users, should be taken into account.
2. Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) models, as well as cryptography in private clouds, do not guarantee privacy. Data security in the private cloud; should be provided by other means such as access control rather than encryption techniques.
3. In the provision of Software as a Service (SaaS) services, cryptographic solutions must be predefined, not on demand, in the provider's contract with the customer.

Conclusion

Alternative solutions to the encryption functionality offered by providers should also be considered, as privacy is clearly required for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). These solutions include the use of encryption services (e.g. key management servers) or encrypted data of pre-cloud storage hosted and managed by a third party (preferably a public department or a trusted security service provider) that enables control over these service models and approves the implementation of encryption processes.

REFERENCES

[1] Compeau DR, Meister DB, Higgins CA. From Prediction to Explanation: Reconceptualizing and Extending the Perceived Characteristics of Innovating. Journal of the Association for Information Systems 2007(8):409–39.

[2] Dillon T, Wu C, Chang E. Cloud Computing: Issues and Challenges. In: Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on: IEEE Computer Society; 2010, p. 27–33.

[3] Gregg DG, Walczak S. Dressing Your Online Auction Business for Success: An Experiment Comparing Two eBay Businesses. MIS Quarterly 2008(32):653–70.

[4] Karahanna E, Agarwal R, Angst CM. Reconceptualizing compatibility beliefs in technology acceptance research. MIS Quarterly 2006(Vol. 30 No. 4):781–804.

[5] Lawkobkit M, Speece M. Integrating Focal Determinants of Service Fairness into Post-Acceptance Model of IS Continuance in Cloud Computing. In: 2012 IEEE/ACIS 11th International Conference on Computer and Information Science; 2012, p. 49–55.

[6] Sonnenwald DH, Maglaughlin KL, Whitton MC (eds.). Using innovation diffusion theory to guide collaboration technology evaluation: work in progress. Enabling Technologies: Infrastructure for Collaborative Enterprises, 2001. WET ICE 2001. Proceedings. Tenth IEEE International Workshops on; 2001.

[7] Tan X, Kim Y. Cloud Computing for Education: A Case of Using Google Docs in MBA Group Projects. In: 2011 International Conference on Business Computing and Global Informatization; 2011, p. 641–644.

[8] Tjikongo R, Uys W. The viability of Cloud Computing Adoption in SMME's in Namibia. In: IST-Africa 2013 Conference Proceedings; 2013, p. 1–11.

[9] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358

[10] Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research and Development Trend. In Second International Conference on Future Networks(ICFN'10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 2010:93–97.CrossRefGoogle Scholar

[11] Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0.. 2011.

[12] Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Verlag Berlin; 2009.

[13] Centre for the Protection of National Infrastructure: Information Security Briefing 01/2010 Cloud Computing. 2010.

[14] Khalid A: Cloud Computing: applying issues in Small Business. International Conference on Signal Acquisition and Processing (ICSAP'10) 2010, 278–28.

[15] Rosado DG, Gómez R, Mellado D, Fernández-Medina E: Security analysis in the migration to cloud environments. Future Internet 2012, 4(2):469–487.

[16] Mather T, Kumaraswamy S, Latif S: Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc.; 2009.

[17] Li W, Ping L: Trust model to enhance Security and interoperability of Cloud environment. In Proceedings of the 1st International conference on Cloud Computing. Beijing, China: Springer Berlin Heidelberg; 2009:69–79.
[18] Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, and Security, CRC Press; 2009.
[18] Kitchenham B: Procedures for perfoming systematic review, software engineering group. Australia: Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd; 2004.
[20] Kitchenham B, Charters S: Guidelines for performing systematic literature reviews in software engineering. Version 2.3 University of keele (software engineering group, school of computer science and mathematics) and Durham. UK: Department of Conputer Science; 2007.
[21] Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M: Lessons from applying the systematic literature review process within the software engineering domain. J Syst Softw2007, 80(4):571–583.
[22] Dahbur K, Mohammad B, Tarakji AB: A survey of risks, threats and vulnerabilities in Cloud Computing. In Proceedings of the 2011 International conference on intelligent semantic Web-services and applications. Jordan: Amman; 2011:1–6
[23] Ertaul L, Singhal S, Gökay S: Security challenges in Cloud Computing. In Proceedings of the 2010 International conference on Security and Management SAM'10. Las Vegas, US: CSREA Press; 2010:36–42.
[24] Grobauer B, Walloschek T, Stocker E: Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 2011, 9(2):50–57.
[25] Subashini S, Kavitha V: A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 2011, 34(1):1–11. 10.1016/j.jnca.2010.07.006
[26] Jensen M, Schwenk J, Gruschka N, Iacono LL: On technical Security issues in Cloud Computing. In IEEE International conference on Cloud Computing (CLOUD'09). 116: 116; 2009:109–116.
[27] Onwubiko C: Security issues to Cloud Computing. In Cloud Computing: principles, systems & applications. Edited by: Antonopoulos N, Gillam L. Springer-Verlag: 2010; 2010.
[28] Morsy MA, Grundy J, Müller I: An analysis of the Cloud Computing Security problem. In Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC; 2010.
[29] Jansen WA: Cloud Hooks: Security and Privacy Issues in Cloud Computing. In Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI. Washington, DC, USA: IEEE Computer Society; 2011:1–10.
[30] Zissis D, Lekkas D: Addressing Cloud Computing Security issues. Futur Gener Comput Syst2012, 28(3):583–592.
[31] Jansen W, Grance T: Guidelines on Security and privacy in public Cloud Computing. Gaithersburg, MD: NIST, Special Publication 800–144; 2011.

الملخص:
اكتسب التطور في نظم المعلومات، الذي حدث على نطاق معين في النصف الثاني من القرن العشرين، زخماً في الربع الأول من القرن الحادي والعشرين؛ جعلت الزيادة السريعة في كثافة وتنوع طلبات المستخدمين، جنبًا إلى جنب مع الابتكارات التكنولوجية والتغييرات في البرامج ومكونات الأجهزة. من الضروري استخدام منهجيات جديدة في معماريات المعلومات. المحاكاة الافتراضية، العمارة الموجهة للخدمة، نموذج الخادم-العميل، الحوسبة الموزعة، إلخ. الحوسبة السحابية، نموذج الخدمة الذي ظهر مع تطوير وتكامل التقنيات والمفاهيم الرائدة؛ توفر هذه الورقة لمستخدميها بنى منخفضة التكلفة ومرنة وقابلة للتطوير ومستقلة عن النظام الأساسي وذات أداء عالٍ، وتهدف هذه الورقة إلى دراسة استراتيجيات اعتماد الحوسبة السحابية من خلال اقتراحات الحلول المتعلقة باستخدام الحوسبة السحابية في المؤسسات العامة.

الكلمات المفتاحية: الإستراتيجيات، الحوسبة السحابية، المنظمات العامة، الحلول، الحلول العملية.