Future Internet **2012**, *4*, 469-487; doi:10.3390/fi4020469

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

Security Analysis in the Migration to Cloud Environments

David G. Rosado [1,*], Rafael Gómez [2], Daniel Mellado [2] and Eduardo Fernández-Medina [1]

[1] GSyA Research Group, Department of Information Systems and Technologies, University of Castilla-La Mancha, Ciudad Real, 13170, Spain; E-Mail: eduardo.fdezmedina@uclm.es

[2] Spanish Tax Agency, Madrid, 28046, Spain; E-Mails: rafael.gomez.lago@gmail.com (R.G.); damefe@esdebian.org (D.M.)

***** Author to whom correspondence should be addressed; E-Mail: david.grosado@uclm.es; Tel.: +34-926-295-300; Fax: +34-926-295-354.

Received: 20 December 2011; in revised form: 23 April 2012 / Accepted: 24 April 2012 / Published: 8 May 2012

Abstract: Cloud computing is a new paradigm that combines several computing concepts and technologies of the Internet creating a platform for more agile and cost-effective business applications and IT infrastructure. The adoption of Cloud computing has been increasing for some time and the maturity of the market is steadily growing. Security is the question most consistently raised as consumers look to move their data and applications to the cloud. We justify the importance and motivation of security in the migration of legacy systems and we carry out an analysis of different approaches related to security in migration processes to cloud with the aim of finding the needs, concerns, requirements, aspects, opportunities and benefits of security in the migration process of legacy systems.

Keywords: security; Cloud computing; migration; legacy system

1. Introduction

Cloud Computing appears as a computational model or paradigm and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources being visualized as services and delivered over the Internet [1,2]. Cloud enhances collaboration, agility, scaling, and availability, the ability to scale to fluctuations in demand, as well as

the acceleration of development work and provides the potential for cost reduction through optimized and efficient computing [3–6].

Cloud computing combines a number of computing concepts and technologies such as SOA, Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while the software and data are stored on the servers [4]. There is commercial pressure on businesses to adopt Cloud computing models but customers need to ensure that their cloud services are driven by their own business needs rather than by providers' interests, which are driven by short-term revenues and sales targets together with long-term market share aspirations [5,7].

The global presence of the Internet and the introduction of wireless networking and mobile devices featuring always on Internet connectivity have raised expectations of users and demand for services over the internet. However, the architectures required by service providers to enable Web 2.0 has created an IT service that is differentiated by resilience, scalability, reusability, interoperability, security and open platform development. This has effectively become the backbone of Cloud computing and is considered by a number of vendors and services to be an operating system layer of its own [5].

The importance of Cloud computing is increasing and it is receiving growing attention in the scientific community. In fact, a study of Gartner [8] has considered Cloud Computing to be the first technology among the top 10 technologies, extremely important and with the best prospect in 2011 and successive years for companies and organizations.

NIST [9] defines Cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Between the essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, highly abstracted resources, near instant scalability and flexibility and measured service. The three service models are Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). Finally, the four deployments models are private cloud, community cloud, public cloud and hybrid cloud [5,9].

In another study about Cloud computing [10] the majority of the participants expect three main drivers of Cloud computing (see Figure 1): more flexibility, followed by cost savings and better scalability of their IT. Cloud computing can bring relief by the faster deployment of applications for less cost. In this same study, an overwhelming majority of participants consider security issues to be their main concern regarding the use of Cloud computing. In addition, legal, privacy and compliance issues are considered to be areas of risks (see Figure 2). Focusing on the security issue, the majority of participants agree that security concerns are blocking their move to the cloud. It appears that they are not worried primarily about the lack of security measures in themselves, but about the lack of transparency on the side of vendors.

The ENISA report [11] highlights the benefits that some small and medium size companies can realize with Cloud computing. A smaller, cost-constrained organization may find that a cloud deployment allows them to take advantage of large-scale infrastructure security measures that they

could not otherwise afford. Some of the possible advantages include DDOS (distributed denial of service) protection, forensic image support, logging infrastructure, timely patch and update support, scaling resilience, and perimeter protection (firewalls, intrusion detection and prevention services).

Figure 1. Benefits of Cloud computing.

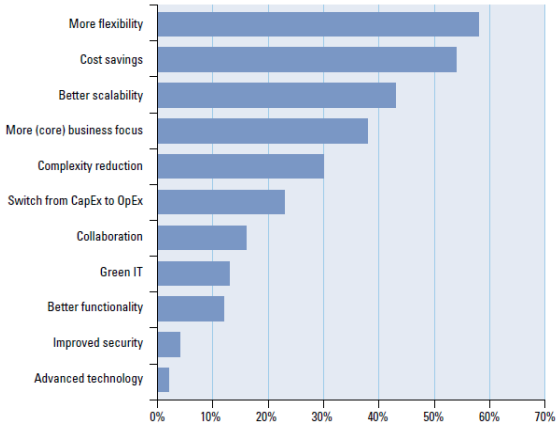
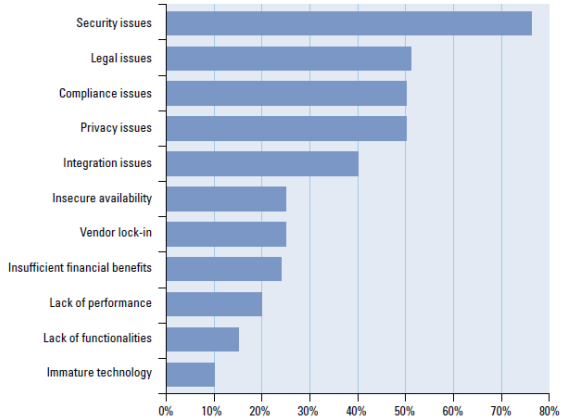


Figure 2. Concerns of Cloud computing.



The adoption of Cloud computing has been increasing for some time and the maturity of the market is steadily growing; not just in volume, choice and functionality, but also in terms of the ability of suppliers to answer the complex security, regulatory and compliance questions that security oversight functions are now asking. In part this growth has been driven by the continued view that cloud services will deliver cost savings and increased flexibility [12].

Legacy information systems typically form the backbone of the information flow within an organization and are the main vehicle for consolidating information about the business. As a solution to the problems these systems pose such as brittleness, inflexibility, isolation, non-extensibility, lack of openness, *etc*., many organizations are migrating their legacy systems to new environments which allow the information system to be more easily maintained and adaptable to new business requirements [13,14].

The essence of legacy system migration is to move an existing, operational system to a new platform, retaining the functionality of the legacy system while causing as little disruption to the existing operational and business environment as possible [15]. Legacy system migration is a very

expensive procedure which carries a definite risk of failure. Consequently before any decision to migrate is taken, an intensive study should be undertaken to quantify the risk and benefits and fully justify the redevelopment of the legacy system involved [13,14].

The need for enterprises to migrate their IT systems to profit from a wide set of benefits offered by Cloud environments. It is not surprising that one of the many opportunities facing established companies in today's competitive environment is how best to leverage the cloud as resource, and by extension how to migrate their existing IT environment into a Cloud. Of particular concern to the CIO are two aspects associated with migration, cost and risk [16]. Security consistently raises the most questions as consumers look to move their data and applications to the cloud. Cloud computing does not introduce any security issues that have not already been raised for general IT security. The concern in moving to the cloud is that implementing and enforcing security policies now involves a third party. This loss of control emphasizes the need for transparency from cloud providers [17]. In some cases the cloud will offer a better security posture than an organization could otherwise provide.

We want to analyze the different existing approaches in the literature about migration processes to Cloud computing while taking into account the security aspects that have to be also moved to Cloud. There are different initiatives that pretend to show the growing importance of migration processes to modernize legacy systems and advance on business needs and services offered by organizations towards an increasing market and for the future. We want to first analyze the different existing proposals to identify and study the most interesting aspects of migration to cloud and then extract the main advantages and disadvantages that exist and identify gaps, challenges and opportunities to be further investigated. In this study we also focus on security issues considered in migration processes as the security in these open environments is very important and has a high value for organizations which wish to move their applications to the cloud.

The remainder of the paper is then organized as follows: Section 2 summarizes the main challenges and benefits of security of Cloud computing. In Section 3 we carry out analysis and review some of the existing proposals of migration to Cloud computing. Then, in Section 4 we discuss and analyze the results of this review. Finally, we present the conclusions and proposals for future work.

2. Security Benefits and Challenges in Cloud Computing

Cloud Computing is not necessarily more or less secure than the current environment although it does create new risks, new threats, new challenges and new opportunities as with any new technology. In some cases moving to the cloud provides an opportunity to re-architect older applications and infrastructure to meet or exceed modern security requirements. At other times the risk of moving sensitive data and applications to an emerging infrastructure might exceed the required tolerance [3].

Although there is a significant benefit to leveraging Cloud computing, security concerns have led organizations to hesitate to move critical resources to the cloud. Corporations and individuals are often concerned about how security and compliance integrity can be maintained in this new environment [7].

With the cloud model, you lose control over physical security due to the fact that you are sharing computing resources with other companies (for public cloud) and moreover, if you should decide to move the storage services provided by one cloud vendor's services to another one, these storage services may be incompatible with another vendor's services. It is recommended that your

development tool of choice should have a security model embedded in it to guide developers during the development phase and restrict users only to their authorized data when the system is deployed into production [7,18].

In the rush to take advantage of the benefits of Cloud computing, not least of which is significant cost savings, many corporations are seemingly rushing into Cloud computing without a serious consideration of the security implications. To overcome the customer concerns about application and data security, vendors must address these issues head-on. There is a strong apprehension about insider breaches, along with vulnerabilities in the applications and systems' availability that could lead to loss of sensitive data and money. Such challenges can dissuade enterprises from adopting applications within the cloud [18]. Therefore, the focus is not upon portability of applications, but on preserving or enhancing the security functionality provided by the legacy application and achieving a successful application migration [3].

The cloud providers and vendors have advanced in this direction improving the security aspects and solutions which are offered to the customers who wish to move their applications and data to cloud, and becoming a very attractive paradigm because of perceived economic and operational benefits.

Among this attractive set of benefits one can find the security benefits which are offered by the cloud providers to their customers who choose to move their applications to the cloud [11,19,20]. Among the most popular security benefits in Cloud computing we can define the following:

- Security and benefits of scale: put simply, all kinds of security measures are cheaper when implemented on a larger scale due to the massive concentration of resources however the data presents a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective. This includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, *etc*.
- Security as a market differentiator: security is a priority concern for many cloud customers; many of whom will make buying choices on the basis of the reputation for confidentiality, integrity and resilience of the provider as well as the security services offered by the provider.
- Standardized interfaces for managed security services: large cloud providers can offer a standardized, open interface to managed security services providers. This creates a more open and readily available market for security services.
- Rapid, smart scaling of resources: the ability of the cloud provider to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, *etc*., to defensive measures (e.g., against DDoS attacks) has obvious advantages for resilience.

In addition to these benefits, Cloud also has others benefits such as being more timely and effective and having efficient updates and defaults. There are some good security traits that come with centralizing your data; Cloud providers have an opportunity for staff to specialize in security, privacy, and other areas of high interest and concern to the organization; the structure of Cloud computing platforms is typically more uniform than that of most traditional computing centers; greater uniformity and homogeneity facilitate platform hardening and enable better automation of security management activities like configuration control, vulnerability testing, security audits, and security patching of platform components resource availability; backup and recovery; and redundancy. Disaster recovery capabilities are built into Cloud computing environments and on-demand resource capacity can be

used for better resilience when facing increased service demands or distributed denial of service attacks, as well as for quicker recovery from serious incidents; the architecture of a cloud solution extends to the client at the service endpoint, used to access hosted applications; data maintained and processed in the cloud can present less of a risk to an organization with a mobile workforce than having that data dispersed on portable computers or removable media out in the field, where theft and loss of devices routinely occur.

3. Security Issues in Public, Private and Hybrid Clouds

While cloud models provide rapid and cost-effective access to business technology, not all of these services provide the same degree of flexibility or security control. In most organizations, data protection levels vary depending on the use of technology [21].

Public clouds (or external clouds) describe Cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications or web services, from an off-site, third-party provider who shares resources and bills on a fine-grained, utility-computing basis. In a public cloud, security management day-to-day operations are relegated to the third party vendor, who is responsible for the public cloud service offering [22].

Private clouds differ from public clouds in that the network, computing, and storage infrastructure associated with private clouds is dedicated to a single organization and is not shared with any other organizations (*i.e.*, the cloud is dedicated to a single organizational tenant). The security management and day-to-day operation of hosts are relegated to internal IT or to a third party with contractual SLAs. By virtue of this direct governance model, a customer of a private cloud should have a high degree of control and oversight of the physical and logical security aspects of the private cloud infrastructure [22].

A hybrid cloud environment consisting of multiple internal and/or external providers is a possible deployment for organizations. With a hybrid cloud, organizations might run non-core applications in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud [22].

Providing security in a private cloud and a public cloud is easier, comparing with a hybrid cloud since commonly a private cloud or a public cloud only has one service provider in the cloud. Providing security in a hybrid cloud consisting of multiple service providers is much more difficult especially for key distribution and mutual authentication. Also for users to access the services in a cloud, a user digital identity is needed for the servers of the cloud to manage the access control. While in the whole cloud, there are many different kinds of clouds and each of them has its own identity management system. Thus a user who wants to access services from different clouds needs to have multiple digital identities from different clouds, which will lead to inconvenience for users. Using federated identity management, each user will have his unique digital identity and with this identity, he/she can access different services from different clouds [23].

4. Approaches of Migration Processes

There are different approaches in which the authors analyze and define migration processes or recommend guides of migration to Cloud computing. Reference [24] defines a set of points to consider when making the decision to migrate a project to an external cloud, which are as follows: (1) Look for

an established vendor with a track record; (2) Does the project really need to be migrated?; (3) Consider data security; (4) Data transfer; (5) Data storage and location; (6) Scaling; (7) Service level guarantees; (8) Upgrade and maintenance schedules; (9) Software architecture; and (10) Check with the lawyers. Other important steps, shown in [25] that can be taken in preparation for Cloud computing adoption are: (i) Identify all potential opportunities for switching from existing computing arrangements to cloud services; (ii) Ensure that in-house infrastructure complements cloud-based services; (iii) Develop a cost/benefit and risk evaluation framework to support decisions about where, when, and how cloud services can be adopted; (iv) Develop a roadmap for optimizing the current ICT environment for adoption of public and/or private cloud services; (v) Identify which data cannot be held in public Cloud computing environments for legal and/or risk-mitigation reasons; (vi) Identify and secure in-house competencies that will be required to manage effective adoption of cloud services; (vii) Designate a cross-functional team to continually monitor which new services, providers, and standards are in this space, and to determine if they affect the roadmap; (viii) Evaluate technical challenges that must be addressed when moving any current information or applications into a cloud environment; (ix) Ensure that the networking environment is ready for Cloud computing. Reference [26] defines the points to take into account in the migration such as (i) Deciding on the applications and data to be migrated; (ii) Risk mitigation; (iii) Understanding the costs; (iv) Making sure the regulatory things are handled; (v) Training the developers and staff. A phased strategy for migration is presented in [27] where the author describe a step by step guide with six steps given as such; (1) Cloud Assessment Phase; (2) Proof of Concept Phase; (3) Data Migration Phase; (4) Application Migration Phase; (5) Leverage of the Cloud; (6) Optimization Phase. In this strategy some security aspects are indicated and some correct security best practices are defined such as safeguard of credentials, restricting users to resources, protecting your data by encrypting it at-rest (AES) and in-transit (SSL) or adopting a recovery strategy. The alternative migration strategies which Gartner [28] suggests IT organizations should consider are: (i) Rehost, *i.e.*, redeploy applications to a different hardware environment and change the application's infrastructure configuration; (ii) Refactor, *i.e.*, run applications on a cloud provider's infrastructure; (iii) Revise, *i.e.*, modify or extend the existing code base to support legacy modernization requirements, then use rehost or refactor options to deploy to cloud; (iv) Rebuild, *i.e.*, Rebuild the solution on PaaS, discard code for an existing application and re-architect the application; (v) Replace, *i.e.*, discard an existing application (or set of applications) and use commercial software delivered as a service.

As we can see, the approaches of migration process identify and define a set of steps or points to follow and consider in the migration to Cloud which can be used for our propose of migrating security aspects to Cloud, but the initiatives do not consider security or only specific security aspects that do not guarantee a full migration process of all security features of the legacy systems and it is this aspect which we want to achieve.

5. Analysis of Approaches of Migration to Cloud

Legacy system migration encompasses many research areas. A single migration project could, quite legitimately, address the areas of reverse engineering, business re-engineering, schema mapping and translation, data transformation, application development, human computer-interaction and testing [15].

Some proposals have been presented in some of these areas such as in [29] where the authors have presented a realistic strategy for conducting migration, by considering both the business needs of the organization and the technical content of the organization's legacy system portfolio. In [30] the authors have mentioned that one of the strategies for migration of legacy systems to SOA is the black box strategy. The wrapping methodology makes interactive functionalities of legacy systems accessible as web services have been discussed in [31]. Finally, a re-engineering approach that is used to restructure legacy system code and to facilitate legacy system code extraction for web service code construction has been proposed in [32].

Sooner or later, enterprises will want to rewrite or replace their legacy applications with those written using a modern architecture, migrate them to the cloud, and manage and control them remotely [33]. Moving critical applications and sensitive data to public and shared cloud environments is of great concern for those corporations that are moving beyond their data center's network perimeter defense. To alleviate these concerns, a cloud solution provider must ensure that customers will continue to have the same security and privacy controls over their applications and services, provide evidence to customers that their organization and customers are secure and that they can meet their service-level agreements, and prove compliance to auditors [7].

Organizations and enterprises are asking how the cloud providers ensure data at rest (on storage devices), how they ensure data in transit, how to authenticate users, how are one customer's data and applications separated from other customers (who may be hackers or competitors), how to address legal and regulatory issues related to Cloud computing, how to respond to incidents and how are customers involved, how the customer and the vendor will respond to incidents in the cloud, who is charged with responding to each type of incident, or if they can conduct forensic investigations to determine what caused an incident. These kind of questions related to security are not clear in Cloud computing and hence organizations and enterprises do not trust the migration of their applications to Cloud environments.

In this section, we have carried out a review of the existing approaches regarding migration to Cloud computing, not only in order to summarize the existing approaches, models, tools, techniques and strategies but also to identify and analyze the security issues considered in these migration approaches with the aim of identifying the possible solutions offered which respond to the security concerns or security needs to be developed or researched. We have carried out a review of the most relevant sources such as Scholar Google, Science@Direct, DBLP, and so on, obtaining a set of approaches that we now believe are most interesting for our analysis and which are detailed as follows.

5.1. Model-Based Migration of Legacy Software Systems into the Cloud: The CloudMIG Approach [34]

This approach presents a specific model for migrating legacy systems into the cloud. It is called the CloudMIG and, in words of their authors, it is still in an early stage. CloudMIG is composed of six activities for migrating an enterprise system to PaaS and IaaS-based cloud environments: (1) Extraction: A model describing the actual architecture of the legacy system is extracted by means of a software architecture reconstruction methodology; (2) Selection: Common properties of different cloud environments are described in a cloud environment meta-model; (3) Generation: The generation activity produces three artifacts, namely a target architecture, a mapping model, and a model

characterizing the target architecture's violations of the cloud environment constraints; (4) Adaptation: The activity 4 allows the re-engineer to adjust the target architecture manually towards case-specific requirements that could not be fulfilled during generation activity 3; (5) Evaluation: This activity evaluates the outcomes of the activities 3 and 4. The evaluation involves static and dynamic analyses of the target architecture; (6) Transformation: This activity comprises the manual transformation of the enterprise system towards the aimed cloud environment according to the generated and improved target architecture.

The approach provides model-driven generation of considerable parts of the system's target architecture and fosters resource efficiency and scalability on an architectural level. The work does not deal with security issues, though the third activity (Generation) provides a model with the target architecture violations of the cloud environment constraints. However, it does not seem to be specific either about security constraints of the legacy or of the target. This approach does not consider security aspects in the process but it would be possible to incorporate some security aspects into each activity in such a way that these aspects would be extracted from the legacy system through the use of a modernization technique or a software architecture reconstruction methodology. A target security architecture could then be generated using a specific cloud environment model together with a security mapping model, and a transformation to secure a migrated system would be possible with this same approach.

5.2. Migrating Legacy Applications to the Service Cloud [35]

The authors present a generic methodology which shows how to migrate legacy applications to the service Cloud computing platform and they describe a case study for scientific software from the oil spill risk analysis domain. This methodology defines seven steps: (1) architectural representation of the legacy: based on the source code and text descriptions, they can analyze the legacy system and reconstruct an architectural model of the legacy application; (2) redesign of the architecture: redesign the original architecture model and in particular identify services that can be provided in a SaaS architecture, specified in a SoaML model; (3) MDA transformation: with MDA transformation technology, they can easily transform the architecture model like SoaML, SysML, UML to target codes like WSDL, JEE Annotation; (4) web service generation: they can generate the target Web service based on the WSDL or JEE Annotation; (5) web service based invocation of legacy functionalities: the service-base application invokes the functionalities from the identified function and service points in the legacy application; (6) selection of the Cloud computing platform: according to the specific requirements of the target system, the most suitable Cloud computing platform will be chosen to support the execution of the Web services; (7) Web service deployment in the service cloud: end users can consume the legacy functionalities through the Web services that run on the cloud.

The paper only deals with security issues in the last step (migration to the cloud). And there it only mentions security in a general non-specific manner, along with scalability and networking. Nor does it appear to provide detailed questioning about the security constraints of the legacy. Nevertheless, this approach could be expanded with security aspects in such a way that the security code of the legacy system could be identified, and an architectural security model of the legacy application could be reconstructed to redesign and identify security services that could be provided in an SaaS architecture,

specified in a SoaML4Security model by carrying out the MDA and MDS (Model Driven Security) transformations and generating Web Service based on WSDL, WS-Security, XACML, SAML, *etc*.

5.3. REMICS-REuse and Migration of Legacy Applications to Interoperable Cloud Services [36]

REMICS (REuse and Migration of legacy applications to Interoperable Cloud Services) is a research project whose main objective is to provide tools for model-driven migration of legacy systems to loosely coupled systems following a bottom up approach; from recovery of legacy system architecture (using OMG's ADM Architecture Driven Modernization) to deployment in a cloud infrastructure allowing further evolution of the system in a forward engineering process. The migration process consists of understanding the legacy system in terms of its architecture, business processes and functions, designing a new Service-Oriented Architecture (SOA) application, and verifying and implementing the new application in the cloud. These methods will be complemented with generic "Design by Service Composition" methods providing developers with tools simplifying development by reusing the services and components available in the cloud.

During the "Migrate" activity, the new architecture of the migrated system will be built by applying specific SOA/Cloud computing patterns and methods like architecture decomposition, legacy components wrapping and legacy components replacement with new discovered cloud services. The migration process will be supported by two complementary activities: "Model-Driven Interoperability" and "Validate, Control and Supervise". The system will be rebuilt for a new platform in a forward MDA process by applying specific transformations dedicated to service Cloud platforms. This work does not deal specifically with security in the migration process but the authors could expand their approach by considering security aspects in the technological approach in parallel, incorporating new activities focused on the extraction of security aspects, the building of a security architecture for the Cloud platform, and the implementation of Cloud security services using some other security techniques such as Model driven Security (MDS) or UMLsec for UML class and deployment diagrams.

5.4. A Benchmark of Transparent Data Encryption for Migration of Web Applications in the Cloud [37]

In this approach the authors analyze privacy requirements for the cloud applications and discuss data encryption approaches for securing ecommerce applications in the cloud. To provide quantitative estimation of performance penalties caused by data encryption, they present a case study for an online marketplace application.

The authors argue that both user related data and critical business transaction data should be encrypted and they examine available encryption approaches on the different layers: The storage layer encryption relies on the encryption of storage devices such as file system and disk or partition encryption; Database layer encryption relies on the encryption functions provided by DBMS. Mainstream databases like Oracle, DB2, MS SQL Server, Mysql offer built-in encryption functions; The middleware layer encryption takes places between front-end applications and backend databases and hides encryption details for the applications; Applications layer encryption, in contrast to middleware layer encryption, requires applications themselves to deal with encryption and decryption of data stored in the database. They compare the advantages and disadvantages of those encryption approaches and, specifically, they recommend middleware layer encryption as the most appropriate

option for migration of legacy ecommerce applications in the cloud, due to its transparency, scalability and vender independency. This approach analyzes privacy requirements for migration of ecommerce applications in the cloud and argues that both user related data and critical business transaction data should be encrypted.

This work is therefore focused on the encryption of data and the transactions of the owners when they migrate their data and applications to Cloud, thus assuring data privacy and providing control of access to the information assets. However, the authors do not indicate any aspect of how the migration should be carried out and what other security aspects should be considered.

5.5. A Case Study of Migrating an Enterprise IT System to IaaS [38]

This approach describes a case study for the migration of a legacy IT system in the oil & gas industry based in the UK. They present the cost analysis they made for the company and the use of a decision support tool to assess migration of businesses into the cloud. This case study identifies the potential benefits and risks associated with the migration of the studied system from the perspectives of: project managers, technical managers, support managers, support staff, and business development staff. The approach is based upon data collected from an IT solutions company when considering the migration of one of their systems to Amazon EC2.

The proposed tool is useful for decision-makers as it helps to address the feasibility challenges of Cloud adoption in enterprises, but this work does not propose any legacy application migration processes, nor does it deal with the security constraints of the legacy applications, and the authors do not consider security as an important point in the migration. Security could be incorporated into this approach by adding a new perspective of security managers and experts and by taking into account a cost analysis for the security necessities of the application for decision-makers so that security is also an important factor in the migration to Cloud.

5.6. Decision Support Tools for Cloud Migration in the Enterprise [39]

This approach describes two tools that aim to support decision making during the migration of IT systems to the cloud. The first is a modeling tool that produces cost estimates for using public IaaS clouds. The tool enables IT architects to model their applications, data and infrastructure requirements in addition to their computational resource usage patterns. The tool can be used to compare the cost of different cloud providers, deployment options and usage scenarios. The second tool is a spreadsheet that outlines the benefits and risks of using IaaS clouds from an enterprise perspective; this tool provides a starting point for risk assessment. Two case studies were used to evaluate the tools. The tools were useful as they informed decision makers about the costs, benefits and risks of using the cloud. The tools were evaluated using two case studies representing a technical system managed by a small team, and a corporate enterprise system. The first case represented a small enterprise that is free from the organizational hierarchy and overheads of large enterprises. The second case study represented a typical enterprise division that has its own independently-managed systems, which are part of a large inter-connected corporate IT environment.

This paper describes one tool for benefit and risk assessment that aims to support decision making during the migration of IT systems to the public IaaS clouds. This provides a starting point for risk

assessment as it outlines the organizational, legal, security, technical and financial benefits and risks of using IaaS clouds from an enterprise perspective. As can be observed, the authors present two support tools (one of which is related to security) for decision making, and they do not propose any migration processes.

5.7. Service Migration in a Cloud Architecture [40]

This approach examines service migration in a Cloud computing environment by examining security and integration issues associated with service implementation. The authors believe that the categories of acquisition, implementation, and security, offer the greatest challenges to service migration in the cloud from the consumer perspective because they represent the slowest and most costly components of the migration problem. They highlight some of the critical problems facing small to medium organizations as they consider cloud computing as a means of obtaining computational services.

The authors consider security as a challenge in the migration service and they take into account issues such as if the user moves to a competing service provider, can you take your data with you? Do you lose access (and control and ownership) of your data if you fail to pay your bill? What level of control over your data do you retain: for example, the ability to delete data that you no longer want? If your data is subpoenaed by a government agency, who surrenders the data? (e.g., who is the target of the subpoena?). If a customer's information is in the cloud, does this violate privacy law? How does an organization determine that a Cloud provider is meeting the security standards it espouses? What legal and financial provisions are made for violations of security and privacy laws on the part of the Cloud provider? Will users be able to access their data and applications without hindrance form the Cloud provider, third parties, or the government?

As we can see, security is treated as an important aspect to take into account in applications once they are migrated to Cloud, but the authors do not propose how these security aspects should be migrated from the legacy applications to Cloud.

5.8. Dynamic Service and Data Migration in the Clouds [41]

The authors propose in this work a framework to facilitate service migration and to design a cost model with the decision algorithm to determine the tradeoffs on service selection and migration. The important issues addressed in this work include that it is necessary to consider the infrastructure support in the cloud to achieve service migration, and that it is also essential to have a strong decision support to help determine whether to migrate some services and where to place them. The authors develop a cost model to correctly capture these costs and help determine the tradeoffs in service selection and migration in clouds.

The important issues addressed in this work include: (1) It is necessary to consider the infrastructure support in the cloud to achieve service migration. The computation resources (computer platforms) in the cloud need to be able to support execution of dynamically migrated services. They develop a virtual machine environment and corresponding infrastructure to provide such support; (2) It is also essential to have a strong decision support to help determine whether to migrate some services and where to place them. The consideration involves the service migration cost, consistency maintenance cost, and the communication cost gains due to migration. They develop a cost model to correctly capture these costs and help determine the tradeoffs in service selection and migration in clouds. Then,

they use a genetic algorithm to search the decision space and make service selection and migration decisions based on the cost tradeoffs.

From a security viewpoint, the authors consider security as a critical issue and they propose mutual authentication and access control among different platforms and services using certificate authority (CA) services to achieve this goal. They define a Security Manager that interacts with CAs and performs service validation, authentication, and authorization. The Security Manager also responds to authentication requests issued by services from other virtual machines (VM). Since VM isolates multiple execution environments and supports the ability to run multiple software stacks with different security levels, they use VM to enforce fine-grained access control to services and local computing platform resources. As will be noted, this approach does not consider security in the migration process, but does consider it in the support infrastructure and to virtual machine level.

6. Results and Discussion

The modernization of state IT legacy systems is emerging as a significant financial, technical and programmatic challenge to the states' ability to deliver services to citizens, and conduct day-to-day business. Although state governments have advanced their IT environment with investments in new technologies, flexible programming and a portfolio of online services, most still live with legacy. Many state systems have become obsolete, difficult to secure and costly to operate and support. Without investments in legacy system renovation, modernization or replacement, the ability of states to operate as a modern organization and serve its citizens is at risk [42].

In order to sum up the results of the systematic review we present in Table 1 a summary of the quantity of studies by initiative. The initiatives are obtained from the main topics found on the approaches analyzed of the review carried out about migration processes to Cloud. The initiatives are if the approaches analyzed define frameworks or methodologies, if these approaches are focused on standards, if they present support tools, if they propose transformations of models in the migration process, if security is considered in these approaches, or if the approaches show a case study. Also, we consider the technology as an initiative when the approaches are focused on Cloud technology, and finally, if the approaches indicate and define meta-models and are based on re-engineering techniques.

All these approaches are interesting from the point view of migration to Cloud which offers methodologies of application, decision tools, meta-models of semi-automated migration with transformations some of them based on MDA, cases of studies of migration with specific technology and specific Cloud providers, and so on, providing interesting aspects to take into account in the migration of legacy systems to Cloud computing. Some of them show how to implement the migration approaches in real applications helped by support tools which giving more credibility and robustness to the proposals analyzed.

However, taking into account the importance of security in Cloud justified with numerous approaches and initiatives in the literature [3,5,11,22,43,44] and that from our point of view and experience, security of legacy systems has to be migrated and even reinforced in the same way as any other aspect, function or service of the system to migrate, we have been surprised. This is because we have not seen this importance and concern in the proposals considered in our review where only some

of them offer security-related issues when making decisions or issues that should be considered when migrating to the Cloud.

Table 1. Overview of studies per topics.

Initiatives	# studies	Frey, S [34]	Zhang,W [35]	Parastoo, M [36]	Hu and Klein [37]	Khajeh-Hosseini [38]	Khajeh-Hosseini [39]	Kaisler, S [40]	Wei Hao [41]
Framework or methodology	4		■	■		■			■
Standards	4		■	■				■	■
Tools	1						■		
Transformations	3	■	■	■					
Security	4				■		■	■	■
Case Study	5		■	■	■	■	■		
Technology	2					■			■
Meta-model and reengineering	1	■							

Organizations moving systems into a cloud environment, or procuring cloud services, may find themselves faced with tough questions on how to ensure security and privacy; the balance between security and cost-effectiveness; the increased availability of systems and the presence of a viable exit strategy [12].

Although there are four initiatives that indicate security aspects to take into account in the migration, none of them presents an approach indicating which are the most important issues to consider, how to perform the migration of these aspects of security, what set of security requirements have to consider, which are the most appropriate mechanisms used to implement certain security services for the Cloud, what security standards are more appropriate taking into account different standards for areas such as healthcare (e.g., Health Insurance Portability and Accountability Act (HIPAA)), finance (e.g., Payment Card Industry Data Security Standard (PCI DSS)), security (e.g., ISO 27001, ITIL, COBIT), and audit (e.g., Standards for Attestation Engagements (SSAE) No. 16) [20], and so on. That is, a migration process to guide and indicate to us the steps, tasks, recommendations, mechanisms, standards, and decisions to follow with the main objective of migrating security aspects and services to the Cloud.

Organizations which want to move to Cloud due to insufficient security infrastructure in its organization or want to add new security services to the systems have clear security benefits, but no one can ensure that the security and privacy levels are equal to or higher than the organizations had in their local systems. Organizations want a complete migration process, offering the same services and even new services improved and provided by Cloud environments but with security level that is the same as if the system was within their own organization. When organizations decide to move to Cloud, they want to migrate their systems and the security of themselves, of course adapted to the new environment. This is achieved with a complete migration process where aspects of security and

security-related decisions are considered and different solutions proposed depending on the level of security required, the scope of the applications and the selected technological providers.

Lack of studies and approaches on security issues in the migration to Cloud is that which we have observed in carrying out this analysis of the literature, where security in Cloud has a great importance. However, there are no initiatives where a migration process is proposed for security aspects, which is very important for an application that provides services in the Cloud.

Therefore, there is an urgent need to provide methodologies, techniques and tools not only for accessing the data and services which is locked in these closed systems and with a high level of security, but also to provide a strategy which will allow the migration of the systems to new platforms and architectures [15] and indicating all security aspects that have to be considered and covered in the migration process.

7. Conclusions

Cloud is growing because cloud solutions provide users with access to high computational power at a fraction of the cost of buying such a solution outright and which can be acquired on demand; the network becomes an important element in the cloud where users can buy what they need when they need it. Although industry leaders and customers have wide-ranging expectations for cloud computing, privacy and security concerns remain a major impediment to widespread adoption.

The benefits of Cloud computing are the first weapon when organizations or companies are considering moving their applications and services to Cloud, analyzing the advantages that it entails and the improvements that they can get. If the customers decide to incorporate their businesses or part of them to the Cloud, they need to take into account a number of risks and threats that arise, the possible solutions that can be carried out to protect their applications, services and data from those risks, and some best practices or recommendations which may be helpful when the customers want to integrate their applications in the Cloud. In addition, organizations or customers require guidelines or processes which indicate the steps necessary and advisable to follow, the techniques most suitable, the most appropriate mechanisms and the technologies to implement the successful migration of all security aspects of their systems to the Cloud, with the purpose of having complete assurance that their systems, data and assets are ensured in the same form as in their own organization or company.

After analysis carried out on such issues in the literature, we can conclude that there are proposals that attempt to migrate legacy applications to the Cloud with some security aspects but they do not bear in mind the security issues to be integrated in their own migration process of legacy systems.

For future work, we will carry out a systematic review of the literature in a formal way, extending the search to migration processes from legacy systems to Cloud computing, searching initiatives of Cloud-related technologies, such as SOA, Web services, Grid or virtual machines, and always considering security aspects in this search. In this way we will obtain more information and we can extract the most important aspects to define a migration process of legacy systems to Cloud taking into account the security aspects within the migration process which have to be migrated as for any other service, requirements or need. Also, we will study the implementation of a legacy application together with a cloud implementation of the same application and we will compare the aspects, functions, services and issues of security which have to be considered in the migration processes. Finally, we will

develop a migration process considering security aspects of the process, adapting and transforming the security components of a legacy application to security services offered by the Cloud.

Acknowledgments

This research is part of the following projects: SERENIDAD (PEII11-037-7035), SISTEMAS (PII2I09-0150-3135) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla- La Mancha" (Spain) and FEDER, and MEDUSAS (IDI-20090557) and PEGASO/MAGO (TIN2009-13718-C02-01) financed by the "Ministerio de Ciencia e Innovación (CDTI)" (Spain).

References

1. Zhao, G.; Liu, J.; Tang, Y.; Sun, W.; Zhang, F.; Ye, X.; Tang, N. Cloud Computing: A Statistics Aspect of Users. In *Proceedings of 1st International Conference on Cloud Computing (CloudCom)*, Beijing, China, 1–4 December 2009; pp. 347–358.
2. Zhang, S.; Zhang, S.; Chen, X.; Huo, X. Cloud Computing Research and Development Trend. In *Proceedings of Second International Conference on Future Networks*, Sanya, Hainan, China, 22–24 January 2010; pp. 93–97.
3. *Security Guidance for Critical Areas of Focus in Cloud Computing*, Version 2.1; Cloud Security Alliance: Palo Alto, CA, USA, 2009.
4. Marinos, A.; Briscoe, G. Community Cloud Computing. In *Proceedings of 1st International Conference on Cloud Computing (CloudCom)*, Beijing, China, 1–4 December 2009; pp. 472–484.
5. Centre for the Protection of National Infrastructure Information Security Briefing 01/2010, 2010. Available online: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf (accessed on 25 April 2012).
6. Khalid, A. Cloud Computing: Applying Issues in Small Business. In *Proceedings of International Conference on Signal Acquisition and Processing*, Bangalore, India, 9–10 February 2010; pp. 278–281.
7. Rittinghouse, J.W.; Ransome, J.F. *Cloud Computing Implementation, Management, and Security*; CRC Press: Boca Raton, FL, USA, 2010.
8. Gartner Home Page. Available online: http://www.gartner.com/it/page.jsp?id=1454221 (accessed on 25 April 2012).
9. The NIST Definition of Cloud Computing. Available online: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (accessed on 25 April 2012).
10. From Hype to Future. KPMG's 2010 Cloud Computing Survey. Available online: http://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Documents/PDF/IT%20Performance/From_Hype_to_Future.pdf (accessed on 25 April 2012).
11. Cloud Computing: Benefits, Risks and recommendations for Information security. Available online: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-interface-2010/presentations/Outlook/Udo%20Helmbrecht_ENISA_Cloud%20Computing_Outlook.pdf (accessed on 25 April 2012).
12. Wilson, P. Positive perspectives on cloud security. *Inf. Secur. Tech.Rep.* **2011**, 16, 97–101.

13. Legacy Information System Migration: A Brief Review of Problems, Solutions and Research Issues. Available online: http://technologycostbestpractices.com/index.php?view=article&id=1957&tmpl=component&print=1&page=&option=com_content 1999 (acessed on 25 April 2012).
14. A Survey of Research into Legacy System Migration. Available online: https://www.scss.tcd.ie/publications/tech-reports/reports.97/TCD-CS-1997-01.pdf (accessed on 25 April 2012).
15. Wu, B.; Lawless, D.; Bisbal, J.; Grimson, J.; Wade, V.; O'Sullivan, D.; Richardson, R. Legacy System Migration: A Legacy Data Migration Engine. In *Proceedings of 17th International Database Conference (DATASEM'97)*, Brno, Czech Republic, 12–14 October 1997; pp. 129–138.
16. Ward, C.; Aravamudan, N.; Bhattacharya, K.; Cheng, K.; Filepp, R.; Kearney, R.; Peterson, B.; Shwartz, L.; Young, C.C. Workload Migration into Clouds—Challenges, Experiences, Opportunities. In *Proceedings of IEEE 3rd International Conference on Cloud Computing*, Miami, Florida, 5–10 July 2010; pp. 164–171.
17. Ahronovitz, M.; Amrhein, D.; Anderson, P.; de Andrade, A.; Armstrong, J; Arasan, B.E.; Bartlett, J.; Bruklis, R.; Cameron, K.; Carlson, M.; *et al*. *Cloud Computing Use Cases White Paper*, 4th ed. Available online: http://socializedsoftware.com/2010/02/17/cloud-computing-use-cases/ (accessed on 4 May 2012).
18. Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1–11.
19. Velte, A.T.; Toby, J. Velte, P.D.; Elsenpeter, R. *Cloud Computing: A Practical Approach*; McGraw-Hill: New York, NY, USA, 2010.
20. Jansen, W.; Grance, T. *Guidelines on Security and Privacy in Public Cloud Computing*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
21. Public clouds, private clouds and your security. Available online: http://www.ibm.com/ibm/files/Z702257B23536P19/15PPCLOUDCOMPUTING_116KB.pdf (accessed on 25 April 2012).
22. Mather, T.; Kumaraswamy, S.; Latif, S. *Cloud Security and Privacy*; O'Reilly Media: Cambridge, MA, USA, 2009.
23. Yan, L.; Rong, C.; Zhao, G. Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. In *Proceedings of 1st International Conference on Cloud Computing—CloudCom'09*, Beijing, China, 1–4 December 2009; pp. 167–177.
24. Holland, R. *Ten Steps to Successful Cloud Migration*; Eagle Genomics Ltd.: Cambridge, MA, USA, 2011.
25. Craig, R.; Frazier, J.; Jacknis, N.; Murphy, S.; Purcell, C.; Spencer, P.; Stanley, J. *Cloud Computing in the Public Sector: Public Manager's Guide to Evaluating and Adopting Cloud Computing*; CISCO Systems, Inc.: San Jose, CA, USA, 2009.
26. Viswanathan, B. Understanding The Cloud Migration Process, 2012. Avaliable online: http://www.cloudtweaks.com/2012/03/understanding-the-cloud-migration-process/ (accessed on 26 April 2012).
27. Varia, J. Migrating your Existing Applications to the AWS Cloud, 2010. Avaliable online: http://media.amazonwebservices.com/CloudMigration-main.pdf (accessed on 26 April 2012).

28. Watson, R. Five Options for Migrating Applications to the Cloud. Avaliable online: http://www.gartner.com/it/content/1448700/1448713/november_17_5_options_cloud_migration_rwatson.pdf (accessed on 26 April 2012).
29. Smith, D. Migration of Legacy Assets to Service-Oriented Architecture Environment. In *Proceedings of International Conference on Software Engineering (ICSE)*, Minneapolis, MN, USA, 20–26 May 2007; pp. 174–175.
30. Zhang, B.; Bao, L.; Zhou, R.; Hu, S.; Chen, P. A Black-Box Strategy to Migrate GUI-Based Legacy Systems to Web Services. In *Proceedings of 4th IEEE International Symposium on Service-Oriented System Engineering*, Jhongli, Taiwan, 18–19 December 2008; pp. 25–31.
31. Canfora, G.; Fasolino, A.R.; Frattolillo, G.; Tramontana, P. Migrating Interactive Legacy Systems to Web Services. In *Proceedings of 10th European Conference on Software Maintenance and Reengineering*, Bari, Italy, 22–24 March 2006; pp. 24–36.
32. Zhang, Z.; Yang, H. Incubating Services in Legacy Systems for Architectural Migration. In *Proceedings of 11th Asia-Pacific Software Engineering Conference*, Busan, Korea, 30 November–3 December 2004; pp. 196–203.
33. Sarna, D.E.Y. *Implementing and Developing Cloud Computing Applications*; CRC Press: Boca Raton, FL, USA, 2011.
34. Frey, S.; Hasselbring, W. Model-Based Migration of Legacy Software Systems into the Cloud: The CloudMIG Approach. In *Proceedings of 12th Workshop on Software-Reengineering of the GI-SRE*, Bad Honnef, Germany, 3–5 May 2010.
35. Zhang, W.; Berre, A.J.; Roman, D.; Huru, H.A. Migrating legacy applications to the service Cloud. In *14th Conference companion on Object Oriented Programming Systems Languages and Applications (OOPSLA 2009)*, Orlando, Florida, USA, 25–29 October 2009; pp. 59–68.
36. Parastoo, M.; Jørgen, B.A.; Sadovykh, A.; Barbier, F.; Benguria, G. Reuse and Migration of Legacy Systems to Interoperable Cloud Services-The REMICS Project. In *Proceedings of 4th Workshop on Modeling, Design, and Analysis for the Service Cloud (MDA4ServiceCloud2010)*, Paris, France, 15 June 2010.
37. Hu, J.; Klein, A. A Benchmark of Transparent Data Encryption for Migration of Web Applications in the Cloud. In *Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, Chengdu, China, 12–14 December 2009; pp. 735–740.
38. Khajeh-Hosseini, A.; Greenwood, D.; Sommerville, I. Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. In *Proceedings of 2010 IEEE 3rd International Conference on Cloud Computing*, Miami, FL, USA, 3–10 July 2010.
39. Khajeh-Hosseini, A.; Sommerville, I.; Bogaerts, J.; Teregowda, P. Decision Support Tools for Cloud Migration in the Enterprise. In *Proceedings of 2011 IEEE 4th International Conference on Cloud Computing*, Washinton, DC, USA, 4–9 July 2011.
40. Kaisler, S.; Money, W.H. Service Migration in a Cloud Architecture. In *Proceedings of 44th Hawaii International Conference on Systems Science (HICSS-44 2011)*, Kauai, HI, USA, 4–7 January 2011, IEEE Computer Society: Washington, DC, USA, 2011; pp. 1–10.

41. Hao, W.; Yen, I.-L.; Thuraisingham, B. Dynamic Service and Data Migration in the Clouds. In *Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference*, Seattle, WA, USA, 20–24 July 2009; IEEE Computer Society: Washington, DC, USA, 2009; pp 134–139.
42. Digital States at Risk!—Modernizing Legacy Systems. Avaliable online: http://www.nascio.org/publications/documents/NASCIO-DigitalStatesAtRisk.pdf (accessed on 26 April 2012).
43. Berger, S.; Cáceres, R.; Goldman, K.; Pendarakis, D.; Perez, R.; Rao, J.R.; Rom, E.; Sailer, R.; Schildhauer, W.; Srinivasan, D.; *et al*. Security for the cloud infrastructure: Trusted virtual data center implementation. *IBM J. Res. Dev.* **2009**, *53*, 1–12.
44. Ertaul, L.; Singhal, S. Security Challenges in Cloud Computing. In *Proceedings of the 2010 International Conference on Security & Management*, Las Vegas, NV, USA, 12–15 July 2010; pp. 36–42.

© 2012 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).