SECURITY APPROACH FOR DATA MIGRATION IN A CLOUD COMPUTING ENVIRONMENT

MARIA KIRAN L
PG Scholar, Dept. of CSE
Cambridge Institute of Technology
Bangalore, India
maria.11cs057@citech.edu.in

PREETHI S
Associate Professor, Dept. of ISE
Cambridge Institute of Technology
Bangalore, India
preethi.ise@cambridge.edu.in

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, data encryption, Cloud computing, data migration, legacy system

I. INTRODUCTION

Cloud computing services such as Amazon EC2 and Windows Azure are becoming more and more popular but it seems many people are still unclear as to what exactly the buzzword "Cloud computing" actually means. In its simplest form, the principle of

Cloud computing is the provision of computing resources via a network.
Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering.

There are many benefits stated of Cloud Computed by different researchers which make it more preferable to be adopted by enterprises.
Cloud Computing infrastructure allows enterprises to achieve more efficient use of their IT hardware and software investments.
This is achieved by breaking down the physical barrier inherent in isolated systems, automating the management of the group of the systems as a single entity. Cloud Computing can also be described as ultimately virtualized system and a natural evolution for data centres which offer automated systems management [3].
Enterprises need to consider the benefits, drawbacks and the effects of Cloud Computing on their organizations and usage practices, to make decision about the adoption and use. In the enterprise, the "adoption of Cloud Computing is as much dependent on the maturity of organizational and cultural (including legislative) processes as the technology, per se" [7].

Many companies have invested in Cloud Computing technology by building their public clouds, which include Amazon, Google and Microsoft. These companies are often releasing new features and updates of their services. For instance Amazon Web Services (AWS) released a Security2 and Economics3 center on their website to have academic and community advice regarding these issues [12]. This shows that there are still lots of doubts about the costs and security for enterprises to adopt Cloud Computing. Hence, the issues of economics and security in Cloud Computing for enterprises must be researched. As large organizations are inherently complex hence, it is very important for Cloud Computing to deliver the real value rather than just be a platform for simple tasks such as application testing or running product demos. For this reason, issues around migrating application systems to the cloud and satisfying the needs of key stakeholders should be explored. The stakeholders include technical, project, operations and financial managers as well as the engineers who are going to be developing and supporting the individual systems. For enterprises economics or cost factor is important but at the same time customer relationships, public image, flexibility, business continuity and compliance are of same importance.

II. DIFFERENT CLOUD PROVIDERS

Cloud services are usually divided in the three main types, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

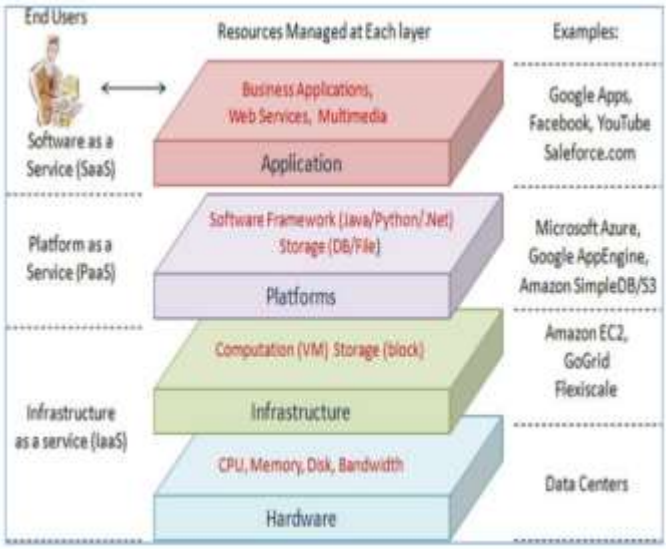

Figure 1: Layered model of Cloud Computing

1. Software as a Service (SaaS): SalesForce. The applications are typically offered to the clients via the Internet and are managed completely by the Cloud provider. That means that the administration of these services such as updating and patching are in the provider's responsibility. One big benefit of SaaS is that all clients are running the same software version and new functionality can be easily integrated by the provider and is therefore available to all clients.

2. Platform as a Service (PaaS): PaaS Cloud providers offer an application platform as a service, for example Google App Engine. This enables clients to deploy custom software using the tools and programming languages offered by the provider. Clients have control over the deployed applications and environment-related settings. As with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider.

3. Infrastructure as a Service (IaaS): IaaS delivers hardware resources such as CPU, disk space or network components as a service. These resources are usually delivered as a virtualization platform by the Cloud provider and can be accessed across the Internet by the client. The client has full control of the virtualized platform and is not responsible for managing the underlying infrastructure.

III. BENEFITS AND CHALLENGES OF SECURITY 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].

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.

IV. SECURITY PROBLEM FOR PUBLIC AND PRIVATE 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].
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].

V. APPROACHES OF MIGRATION PROCESSES

There are different approaches in which the authors analyse 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.

VI. PROPOSED SOLUTION OF SECURING DATA MIGRATION PROCESS

We have talked about security in cloud computing many times before, explaining why it is just as safe as conventional networking security, even citing its benefits over the conventional. However, there are many who still find cloud computing security lacking.
Individuals who still worry about cloud security are those that fall under the financial institution category like banks, brokers, lenders and the like. They do not trust third party cloud computing providers and vendors, at least not with their most sensitive information and data. They might use cloud computing for some things like websites and applications that they think they can risk security with, but they would never consider parting with direct access of their financial and other similar data.
The process of transitioning all or part of a company's data, applications and services from on-site premises behind the firewall to the cloud, where the information can be provided over the Internet on an on-demand basis. While a cloud migration can present numerous challenges and raise security concerns, cloud computing can also enable a company to potentially reduce capital expenditures and operating costs while also benefiting from the dynamic scaling, high availability, multi-tenancy and effective resource allocation advantages cloud-based computing offers.

1. 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 artefacts, 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.

2. Transparent Data Encryption for Migration of Web Applications in the Cloud [37]

In this approach the authors analyse 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 and 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 analyses 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.

3. 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.

4. 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 modelling 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. Prediction based Encryption (PBE) [19]

Predicate Based Encryption (PBE), represents a family of asymmetric encryption schemes that allows for selective fine-grained access control as part of the underlying cryptographic operation. The origins of PBE are in Identity Based Encryption (IBE). In IBE schemes an entity's encryption key is derived from a simple string that represents the entity's own public identity e.g. an email address. For example, given an entity “Virendra” his corresponding encryption key will be during encryption, the resulting cipher-text will effectively be labelled with the string representing the encryption key, the entity's public identity. An entity's decryption key will be derived from the same string used for the encryption key e.g. Virendra's decryption key will be derived from his e-mail address. On receipt of a cipher text message the recipient will be able to decrypt the cipher-text if and only if the two identities, contained within the decryption key and cipher-text, are `equal'. PBE schemes offer a richer scheme in which an entity's `identity' can be constructed from a set of attributes and decryption is associated with access policies that offers a more expressive means with which to describe the relation between the attributes.

A solution might be Prediction Based Encryption (PBE) for multicasting. PBE is a combination of both IBE (Identity Based Encryption)[19][20] and ABE (Attribute Based Encryption) [22][24]. In this work, the attributes are used to design user's decryption keys and to encrypt simple text messages. Decryption occurs when a match occurs between the attributes held by the entity (in their Decryption key) and the attributes used to construct a simple text. This matching occurs through the use of predicates, which describe:

- The required attributes needed to decrypt
- The relationship between the attributes.

PBE scheme supports four operations allowing for encryption, decryption and key generation. The precise value for encryption and decryption keys is dependent upon both the construction of the scheme and placement of predicates. A general PBE scheme consists of the four operations [18]:

- **Setup:** initializes the crypto-scheme and generates a master secret key MSK, used to generate decryption keys, and a set of public parameters MPK.

(MSK, MPK):=Setup ()

- **KeyGen:** generates a decryption key Dec (entity) based upon the master secret key and some entity supplied input.

Dec (entity):=KeyGen (MSK, input)

 Encrypt: encrypts a plain-text message M using the public parameters and supplied encryption key for an entity.

CT: = Encrypt (M, MPK, Enc (entity))

 Decrypt: decrypts a cipher-text if and only if the attributes held by the entity can satisfy the access policy.

M: = Decrypt (CT, MPK, Dec (entity))

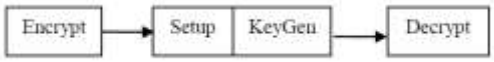

Figure 2. Functioning of the proposed system

Sr. No	Year	Paper Title	Proposed Algorithm	Pros	Cons	Future Gap
1.	2018	Evaluating cloud data base migration options using workload models	DBL Modeller + Mig Sim + OLTP	Zero down time	Complex for relational to relational data base migration	Random values can be used to check database capacity. No support to relational migrations and Automating cost models.
2.	2018	Data migration in cloud computing using homey encryption	Homey encryption cryptographic algorithm	CIA goals	Used in virtual World	Real world implementation can be done
3.	2018	Optimization of stream-based live data migration strategy in the cloud	Live data migration strategy with (PSO) particle swarm optimization, and non-linear migration cost and balance model	Parallel execution	Not for large-scale and to stream data. Need clustering algorithm	Need of improving grouping PSO. And iterative algorithm
4.	2017	Using Homomorphic Encryption to Compute Privacy Preserving Data Mining in a Cloud Computing Environment	Closed patterns using homeomorphic algo Dist-CLOSE algorithm in a distributed environment	less communication and computation overhead	Protect the confidentiality of data	Strengthening the ways to exchange data between the sites
5.	2017	A Risk Management Framework for Cloud Migration Decision Support	Risk management framework	Identify + Manage risks	Complex for large values	Can be made efficient for random values
6.	2017	Information Technology Infrastructure Library and the migration to cloud computing	ITIL + CC Migration Framework	Manage + support Better usability and ease	Need of expertise and implemented in Virtual world	Real world implementation used to define, analyze and map in ITIL

TABLE 1. Overview of Studies per Methods.

VII. CONCLUSION

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, analysing 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.

VIII. FUTURE WORK

The future work can be carried out the optimization of security work as an idea to ensure about the work reliability. With the help of LP (Linear Programming), we will optimize the secured data.

IX. 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. Availableonline: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. Availableonline: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] C. Schridde, T. Dornemann, E. Juhnke, B. Freisleben, M. Smith, "An Identity-Based Security Infrastructure for Cloud Environments," 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), pp. 644 – 649, 2010.

[20] J. Y. Sun, C. Z, Y. C. Zhang, and Y. G. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks, "IEEE Transactions on Parallel and Distributed Systems, vol. 21, no.9, pp. 1227-1239, 2010.

[21] A Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Advances in Cryptology - EUROCRYPT 2010. Springer, 2010.

[22] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," Journal of Computer Security, vol. 18, no. 5, pp. 799–837, 2010.

[23] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-based access control in social networks with efficient revocation," in ASIACCS, Hong Kong, March 2011.

[24] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.

[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:

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[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] 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.