%% The openany option is here just to remove the blank pages before a new chapter

\documentclass[12pt,oneside]{first}

\title{Critical analysis of vendor lock-in }

\usepackage{pagenote}

\usepackage{graphicx}

\usepackage{times}

\usepackage{ragged2e}

\usepackage[ruled,vlined]{algorithm2e}

\usepackage[noend]{algpseudocode}

\usepackage{algorithm}

\usepackage{algorithmic}

\usepackage{lineno}

\usepackage{amsmath}

\usepackage{amsthm}

\usepackage{amssymb}

\usepackage{fancyhdr}

\pagestyle{fancy}

\fancyhf{}

\fancyhead[LE,RO]{\textit{\leftmark}}

\fancyhead[RE,LO]{\textit{ vendor lock-in}}

\fancyfoot[LE,LO]{\textit{Federal Institute of Science and Technology}}

\fancyfoot[LE,RO]{\thepage}

\renewcommand{\headrulewidth}{1pt}

\renewcommand{\footnotesize}{8pt}

\renewcommand{\footrulewidth}{1pt}

\title{Critical analysis of vendor lock-in and its

impact on cloud computing}

\author{ADARSH B S}

\begin{document}

\onehalfspacing

\maketitle

\makeack

\newpage

\pagestyle{empty}

\pagenumbering{gobble}

\begin{center}

\bf \Large ACKNOWLEDGMENT

\end{center}

\subparagraph{} \large First and foremost, I praise and thank God Almighty, who made all circumstances favorable for the completion of this Seminar. Apart from the efforts put in by me, the success of this seminar depends on the encouragement and guidelines of many others. \textbf{Mr. Paul Mundadan}, Chairman, FISAT Governing Body, who provided me with the vital facilities required by the seminar right from inception to completion.

\subparagraph{} \large I express my sincere thanks and gratitude to \textbf{Dr.K S M Panicker}, Director, Academics, FISAT for his immense support. \textbf{Dr. George Issac}, Principal, FISAT, for the amenities he provided, which helped us in the fulfillment of the seminar. \textbf{Mr. Santhosh Kottam J.C.}, HOD(MCA Dept.), FISAT, who always guided me in all phases of my seminar.

\subparagraph{} \large I also thank \textbf{Ms. Manju Joy} for her supervision and also for her support in completing the seminar. The faculty of the MCA department, FISAT, and Lab Instructors for providing me with the necessary Lab facilities and helping us throughout this seminar. My family who inspired, encouraged and supported me in every trial that came our way. I thank them for giving me not just financial, but moral and spiritual support.

\newpage

\pagestyle{empty}

\pagenumbering{gobble}

\begin{center}

\bf \LARGE ABSTRACT

\end{center}

\large \justify Vendor lock-in is a major barrier to the adoption of cloud computing, due to the lack of standardization. Current

solutions and efforts tackling the vendor lock-in problem are predominantly technology-oriented. Limited studies

exist to analyse and highlight the complexity of vendor lock-in problem in the cloud environment. Consequently,

most customers are unaware of proprietary standards which inhibit interoperability and portability of applications

when taking services from vendors. This paper provides a critical analysis of the vendor lock-in problem, from a

business perspective. A survey based on qualitative and quantitative approaches conducted in this study has

identified the main risk factors that give rise to lock-in situations. The analysis of our survey of 114 participants

shows that, as computing resources migrate from on-premise to the cloud, the vendor lock-in problem is

exacerbated. Furthermore, the findings exemplify the importance of interoperability, portability and standards in

cloud computing. A number of strategies are proposed on how to avoid and mitigate lock-in risks when migrating

to cloud computing. The strategies relate to contracts, selection of vendors that support standardised formats and

protocols regarding standard data structures and APIs, developing awareness of commonalities and dependencies

among cloud-based solutions. We strongly believe that the implementation of these strategies has a great potential

to reduce the risks of vendor lock-in.

\justify

\newpage\thispagestyle{empty}

\tableofcontents

\newpage\thispagestyle{empty}

\listoffigures

\newpage\thispagestyle{empty}

\newpage

\pagestyle{fancy}

\pagenumbering{arabic}

\chapter{INTRODUCTION}

Cloud computing allows you to access your data and programs outside of your own computing environment. Rather than storing your data and software on your personal computer or server, it is stored in 'the cloud'. This could include applications, databases, email and file services .Cloud computing provides a way for your business to manage your computing resources online. The term has evolved over recent years, and can be used to describe the use of a third party for your storage and computing needs. The 'cloud' refers to the internet, and operating 'in the cloud' describes the way you store and access your data through an internet connection. Cloud computing allows businesses to access their information virtually, creating a flexible and global way of accessing your data any place, any time. \subparagraph{}The vendor lock-in problem in cloud computing is the situation where customers are dependent (i.e. locked-in) on a single cloud provider technology implementation and cannot easily move in the future to a different vendor without substantial costs, legal constraints, or technical incompatibilities . In the consumer market we see people using a variety of cloud services from different vendors , for example Flickr to share pictures, Gmail to read email, Microsoft to chat, Twitter to Tweet etc. The complexities of cloud service migration mean that many customers stay with a provider that doesn’t meet their needs, just to avoid the cumbersome process. To move data from one provider’s cloud environment to another, for example, it’s often necessary to first move the data back to the customer’s site and then move it to the new provider’s environment. Furthermore, the data may have been altered for compatibility with the original provider’s system so that what is returned to the customer needs to be returned to its former state before it can be moved again.

\chapter{FOUR DIMENSIONS OF LOCK-IN

}

\begin{enumerate}

\item Horizontal lock-in\\

This restricts the ability to replace a product with a comparable or competitive product. If I choose solution A (let’s for example take a CRM solution or a development platform), then I will need to migrate my data and/or code, retrain my users and rebuild the integrations to my other solutions if I want to move to solution B

\item Vertical lock-in\\ This restricts choice in other levels of the stack and occurs if choosing solution A mandates use of database X, operating system Y, hardware vendor Z and/or implementation partner S. To prevent this type of lock-in the industry embraced the idea of open systems, where hardware, middleware and operating systems could be chosen more independently.

\item Diagonal (of inclined) lock-in\\ This is a tendency of companies to buy as many applications as possible from one provider, even if his solutions in those areas are less desirable. Companies picked a single vendor to make management, training and especially integration easier but also to be able to demand higher discounts

\item Generational lock-in\\ This last one is as inescapable as death and taxes and is an issue even if there is no desire to avoid horizontal, vertical or diagonal lock-in. No technology generation and thus no IT solution or IT platform lives forever (well, maybe with exception of the mainframe). The first three types of lock-in are not too bad if you had a good crystal ball and picked the right platforms (eg. Windows and not OS/2) and the right solution vendors (generally the ones that turned out to become the market leaders). But even such market leaders at some point reach end of life. Customers want to be able to replace them with the next generation of technology without it being prohibitively expensive or even impossible because of technical, contractual or practical lock-in.

metadata stored by the cloud database are always encrypted.

\end{enumerate}

\chapter{TYPES OF VENDOR LOCK-IN RISKS}

The issue with vendor lock-in is the difficulty in moving to another cloud service provider if something goes awry. You hope that this never has to happen, but it’s a possibility.

There are four primary lock-in risks that you’ll take working with a single cloud provider. These include:

\begin{enumerate}

\item Data transfer risk

\item Application transfer risk

\item Infrastructure transfer risk

\item Human resource knowledge risk

\end{enumerate}

\begin{enumerate}

\item Data transfer risk\\ It is not easy to move your data from one CSP to another.

A myriad of questions will arise during a data migration process, such as:

1. Who is responsible for extracting the data from the cloud databases and data warehouses?

2. In what format will the data be? Will that format work with the new cloud provider, or will significant changes need to be made to the data?

3. How can the data be transferred without loss of application functionality?

4. How long will it take and how much will it cost to move all of this data?

While some industry groups have tried to create standards for data interchange, sometimes it’s difficult for companies to implement them due to their unique business requirements.

\item Application transfer risk\\If you build an application on one CSP that leverages many of its offerings, the reconfiguration of this application to run natively on another provider can be an extremely expensive and difficult process.

For instance, let’s say you’ve developed a business intelligence platform on Microsoft Azure. You leverage basic cloud services like compute, storage, databases, and networking. But the app also includes Azure’s machine learning, data lake analytics, and bot services.

\item Infrastructure transfer risk\\Every major CSP does things a little bit differently.

Virtual machine formats and their associated pricing vary from vendor to vendor, making it difficult to ensure that you have the appropriate resource usage and cost savings if you switch providers.

Database offerings and formats may differ as well.

And one cloud provider may have more attractive offerings in certain infrastructure components, while lacking in other services that you may need.

These differences in the underlying infrastructure result in difficulties moving from one cloud service provider to another.

\item Human resource knowledge risk\\If you’ve been working with a single CSP, your IT team has likely gained a lot of institutional knowledge about that provider’s tools and configurations.

If you have to move your applications to another CSP, it will take time for your engineers to ramp up their knowledge of the new cloud platform. They’ll have to learn about new infrastructure formats, implementation processes, and more.

\end{enumerate}

\chapter{FACTORS

}

\subparagraph{FACTORS THAT CONTRIBUTE TO A LOCK-IN SITUATION

IN CLOUD COMPUTING} To explore factors that contribute to a lock-in situation in cloud computing, epistemologically, our study design in this paper consists of two distinct phases

\begin{figure}[h!]

\centering

\includegraphics[height=5cm,width=11cm]{1.jpg}

\caption{two phase exploratory research design.}

\end{figure}

\begin{enumerate}

\item \textbf{pilot interview study}\\In the pilot study, qualitative data were collected through the use of open-ended interviews with IT practitioners to explore the business-related issues of vendor lock-in affecting cloud adoption. Five participants from different industry sectors and organiza}tions were purposely selected for in-depth interviews. They included a security expert, cloud advisor, IT technician, business end user, and an IT manager. The purpose was to explore the cloud lock-in problems, and explore the prevalence of its dimensions, by gaining a range of insights from different IT professionals.

\subparagraph{} Seven themes emerged in relation to participants’ perception of vendor lock-in problem and how this affects their migration and adoption decisions. The themes were; (1) standards, (2) interoperability in the cloud environment, (3) the need for portability, (4) integration challenges, (5) contract exit strategy, (6) data ownership (7) security and privacy issues. The analysis of the responses across the seven themes showed the participants’ priority of the themes. As a result, data portability and interoperability concerns were the most discussed theme in relation to vendor lock-in. However, participants were less interested to divulge about the security and contract exit strategies, including data ownership and privacy risks. Subsequent to the pilot interviews a questionnaire was designed for a survey. The main issues raised at the interviews were incorporated into the questionnaire.

\item quantitative survey questionnaire\\

The goal of phase 2 was to identify and evaluate the risks and opportunities of vendor lock-in which affect stakeholders’ decision-making about adopting cloud solutions. This phase of the research design is based on an online survey tool [38]. Participants were selected and invited by e-mail to participate in the survey. The aim of the survey was an in-depth study of the effect of vendor lock-in in migration of enterprise IT resources to the cloud.

\end{enumerate}

\begin{figure}[h!]

\centering

\includegraphics[height=8cm,width=11cm]{2.jpg}

\caption{Sample profile of participants.}

\end{figure}

\chapter{Findings}

\subparagraph{} The analysis of the results show over 49 \% of top level

IT managers influence the decisions for adopting cloud

services. This confirms that cloud computing adoption

in the UK is seen as a viable IT deployment model.

Moreover, more than half (50.9 \%) of the organisations

polled in the study are already using cloud services for

at least one application domain within their organisation.

The higher majority (69 \%) utilise a combination of

cloud services and internally owned applications (i.e. hybrid

IT) for organisation’s needs

\begin{figure}[h!]

\centering

\includegraphics[height=8cm,width=11cm]{3.png}

\caption{Cloud adoption maturity in UK.}

\end{figure}

\section{The business benefits of cloud migration}

\begin{figure}[h!]

\centering

\includegraphics[height=8cm,width=11cm]{4.jpg}

\caption{Benefits of cloud computing to UK Enterprises.}

\end{figure}

\subparagraph{}

\begin{itemize}

\item The majority of the respondents identified capacity and scalability (70.3 \%), increased collaboration,availability, geography and mobility as benefits for migration.

\item This indicates that the business benefits of migrating to the cloud vary across different organisation sizes.

\end{itemsize}

\newpage

\section{Challenges to cloud implementation for UK businesses}

\begin{figure}[h!]

\centering

\includegraphics[height=8cm,width=11cm]{5.jpg}

\caption{Barriers to cloud implementation in the UK.}

\end{figure}

\begin{itemize}

\item The main question here is “what are the greatest barriers for implementing cloud computing for organisations?”

\item Data security risks, loss of control and over dependence on a single cloud provider (35.1 \%) as core existing barriers to future cloud implementation.

\item (48.6 \%) participants are concerned about lack of trust.

\end{itemize}

\endsection

\newpage

\section{Vendor lock-in concerns and challenges in cloud migration}

\begin{figure}[h!]

\centering

\includegraphics[height=8cm,width=11cm]{6.jpg}

\caption{Barriers to cloud implementation in the UK.}

\end{figure}

\begin{itemize}

\item As cloud computing adoption rate soars across the UK market, the risks of vendor lock-in is also prevalent.

\item has the risks of data breach and cyber-attack, or failure to meet agreed service levels.

\item UK businesses are also concerned about having corporate data locked-in to a single cloud provider.

\end{itemize}

\endsection

\newpage

\section{Minimize lock-in risks in cloud migration}

\begin{figure}[h!]

\centering

\includegraphics[height=8cm,width=11cm]{7.jpg}

\caption{Practical challenges of vendor lock-in in cloud migration.}

\end{figure}

\begin{itemize}

\item UK businesses provide effective and efficient strategies to manage lock-in risk(s)

\item The main strategies:

\begin{enumerate}

\item making well-informed decisions before selecting vendors and/or signing cloud contracts (66.4 \%)

\item the need for an open environment for continuous competition between providers in the cloud service market (52.3 \%)

\item use of standard software components with industry-proven interfaces (39.3 \%).

\end{enumerate}

\end{itemize}

\chapter{STEPS TAKE TO AVOID VENDOR LOCK-IN}

The risks that you take with having all your data, applications, and infrastructure with one cloud provider seem ominous. But there are a few things that you can do to ensure that your vendor lock-in risk is minimized.

\section{Do your due diligence}

Before you select your CSP, you should thoroughly vet that they will give you everything that you need to run your applications reliably.

Your CSP selection process should look something like this:

\begin{enumerate}

\item Determine your goals of migrating to the cloud

\item Assess your current IT situation, including a thorough audit of your current infrastructure and cost and resources levels

\item Select the type of cloud environment needed – public, private, or hybrid?

\item Determine the specific cloud components necessary

\item Choose the right cloud provider for your situation

\end{enumerate}

You should consider all of the CSPs’ offerings to see if they match your needs, look at the different pricing models to determine the cost savings you can realize, understand their service level agreements, consider their data transfer processes and costs, and get to know other companies similar to yours with whom they’ve worked.

A deep understanding of your potential CSP is critical in mitigating the risk of vendor lock-in.

\section{Plan early for an exit}

It’s kind of like a cloud pre-nuptial agreement.

It might be weird to plan for an exit before you even “get married” to your cloud provider, but it’s an important step to protect your company in case things go south.

While you plan your implementation strategy, include an exit plan and potential costs. And don’t plan out further than a couple of years; doing so may hamper your flexibility in migrating to another CSP if things go wrong.

\section{Design your application to be loosely coupled}

To minimize the risk of vendor lock-in, your applications should be built or migrated to be as flexible and loosely coupled as possible.

Cloud application components should be loosely linked with the application components that interact with them.

You can do this by incorporating REST APIs with popular industry standards like HTTP, JSON, and OAuth to abstract your applications from the underlying proprietary cloud infrastructure.

Also, any business logic should not only be separated from the application logic, but should be clearly defined and documented. This will avoid the need to decipher business rules in case a migration to a new CSP occurs.

Not only does this reduce the level of lock-in to a single vendor, but it also gives your application interoperability that’s required for fast migration of workloads and multi-cloud environments (more on this later).

\begin{figure}[h!]

\centering

\includegraphics[height=8cm,width=11cm]{8.png}

\caption{Tightly and loosely coupled apps.}

\end{figure}

\section{Maximize portability of your data}

Data is one of the biggest sticking points in cloud migrations, as different formats and models can cause portability issues.

The Open Data Element Framework was created to help standardize the documentation, categorization, and indexing of data, and the Cloud Data Management Interface helps define how to create, retrieve, update and delete data elements from the cloud.

Unfortunately these standards aren’t always well understood, accepted, nor applied.

To maximize the portability of your data, avoid proprietary formatting. Describe data models as clearly as possible, using applicable schema standards to create detailed computer- and human-readable documentation.

Additionally, you should ensure that your cloud provider provides a way for you to extract data easily and economically.

\section{Consider a multi-cloud strategy}

More businesses are moving to a multi-cloud environment, where you can leverage multiple CSPs to power your applications.

For example, you might use Amazon EC2 for your compute power and Redshift for your data warehouse while using IBM Bluemix’s Watson as your artificial intelligence platform.

By going multi-cloud, you become less dependent on one CSP for all of your needs. Another benefit is that you can cherry-pick offerings from each cloud provider so you can implement best-of-breed services into your applications.

There are some cons to a multi-cloud approach, such as an increased burden on development teams, more security risk, and others. (See here for an in-depth list of the pros and cons of multi-cloud environments.)

But you may find that it’s a viable option to mitigate vendor lock-in.

\chapter{ DevOps tools}

Issues with cloud lock-in surpass those of technical incompatibility and data integration. Mitigating cloud lock-in risks cannot be guaranteed with a selection of individual open (technology-centric) solutions or vendors. Instead, the management and operation of cloud services to avoid lock-in should be addressed at a standardised technology-independent manner. In this respect, we present a concise discussion on the potential of DevOps and of tools (such as Chef, Juju and Puppet) that support interoperable management.

DevOps is an emerging paradigm to eliminate the split and barrier between developers and operations personnel. Automation underlies all the practices that constitute DevOps. The philosophy behind DevOps is to bring agile methodologies into IT infrastructure and service management [65]. This is achieved by implementing the concept of “Infrastructure as Code” (IaC) using configuration management tooling. An automation platform is what provides the ability to describe an infrastructure as code.

\newpage

\begin{enumerate}

\item Chef

\subparagraph{}

Chef is a configuration management framework written in Ruby . Chef uses an internal Domain Specific Language or DSL to express configurations. Configuration definitions (i.e. ruby-scripts) and supporting resources (e.g. installation files) in Chef are called recipes. These recipes are basically scripts written in DSL to express the target state of a system . Chef manages so called nodes. A node is an element of enterprise infrastructure, such as a server which can be physical, virtual, in the cloud, or even a container instance running a Chef client . Chef provides APIs to manage resources on a machine in a declarative fashion. Chef recipes are typically declarative (resources which define a desired state) but can include imperative statements as well. Combining a Chef system together with cloud infrastructure automation framework makes it easy to deploy servers and applications to any physical, virtual, or cloud location.

\item Puppet

\subparagraph{}

Puppet is an open source configuration and management tool implemented in Ruby that allows expressing in a custom declarative language using a model-based approach . Puppet enables deploying infrastructure changes to multiple nodes simultaneously. It functions the same way as a deployment manager, but instead of deploying applications, it deploys infrastructure changes. Puppet employs a declarative model with explicit dependency management. One of the key features of Puppet is reusability. Modules can then be reused on different machines with different operating systems. Moreover, modules can be combined into configuration stacks

\item juju

\subparagraph{}

Juju is a cloud configuration, deployment and monitoring environment that deploy services across multiple cloud or physical servers and orchestrate those services . Activities within a service deployed by Juju are orchestrated by a Juju charm, which is a deployable service or application component .

\subparagraph{}

In summary, as applications evolve to function in the cloud, organizations must reconsider how they develop, deploy, and manage them. While cloud computing is heavily used to provide the underlying resource, our review shows that DevOps tools and artefacts can be used to configure and manage these resources. As a result, end-to-end deployment automation is efficiently enabled by employing DevOps approaches in cloud environments. But, cloud providers such as Amazon and cloud frameworks such as OpenStack provide cost-effective and fast ways to deploy and run applications. However, there is a large variety of deployment tools and techniques available . They differ in various dimensions, most importantly in the metamodels behind the different approaches. Some use application stacks (e.g., AWS OpsWorks2 or Ubuntu Juju) or infrastructure, others use lists of scripts (e.g., Chef run) or even PaaS-centric application package descriptions such as Cloud Foundry manifests.

\end{enumerate}}

\chapter{Discussion and conclusion}

\large

In this paper a comprehensive analysis of vendor lock-in problems was discussed and the impact to companies as a result of migration to cloud computing was explored. A survey was conducted and revealed that the cloud paradigm has greatly impacted on many organisations subsequent to migrating IT and business applications to the cloud due to vendor lock-in. In fact, the study has shown that, while organisations are eager to adopt cloud computing due to its benefits, there is equally an urgent need for avoiding vendor lock-in risks. Moreover, the results of our study have highlighted customers’ lack of awareness of proprietary standards which prohibit interoperability and portability when procuring services from vendors.

\para

Therefore, we propose the following strategic approaches to address the issues: (i) create awareness of the complexities and dependencies that exist among cloud-based solutions; (ii) assess providers’ technology implementation such as API and contract for potential areas of lock-in; (iii) select vendors, platforms, or services that support more standardised formats and protocols based on standard data structures; and (iv) ensure there is sufficient portability. In our future work, we will explore interoperability and portability constraints which affect enterprise application migration and adoption of SaaS clouds.

\chapter{REFERENCES}

\begin{itemize}

\item https://www.ca.com/en/blog-highlight/the-concept-of-vendor-lock-in-and-how-it-relates-to-cloud-computing.html

\item http://farm5.static.flickr.com/4099/4793016614\_946f75f082.jpg

\item https://www.thorntech.com/2017/09/avoidingcloudvendorlockin/

\item H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra. " ExecutingSQL over Encrypted Data in the Database-Service-Provider Model." Proc. ACM SIGMOD Int' l Conf.

Management Data, June 2002.

\item M. Hadavi, E. Damiani, R. Jalili, S. Cimato, and Z. Ganjei, " AS5: A Secure Searchable Secret Sharing Scheme for Privacy Preserving Database Outsourcing." Proc. Fifth

Int' l Workshop Autonomous and Spontaneous Security, Sept. 2013.

-

\end{itemize}

\end{document}