A SECURE CLOUD MIGRATION FRAMEWORK FOR CLOUD COMPUTING

A Thesis by

Jainish Rajesh Jain

Bachelor of Engineering, Jain University, 2014

Submitted to the Department of Electrical Engineering and Computer Science
and the faculty of the Graduate School of
Wichita State University
in partial fulfillment of
the requirements for the degree of
Master of Science

December 2017

A SECURE CLOUD MIGRATION FRAMEWORK FOR CLOUD COMPUTING

The following faculty members have examined the final copy of this thesis for form and content, and recommend that it be accepted in partial fulfillment of the requirement for the degree of Master of Science with major in Computer Science.

_____

Abu Asaduzzaman, Committee Chair

_____

Krishna Krishnan, Committee Member

_____

Chengzong Pang, Committee Member

_____

M. Edwin Sawan, Committee Member

"Work Hard in Silence and let your Success be the noise"

ACKNOWLEDGEMENT

I would like to thank Wichita State University for giving me such a wonderful opportunity to perform this thesis work. Many thanks to my advisor, Dr. Abu Asaduzzaman, who deserves special mention here and without whom I would not have completed this work. I am highly indebted to him for his keen guidance, knowledge, and direction towards the completion of my thesis. I also thank Dr. Krishna Krishnan, Dr. M. Edwin Sawan and Dr. Chengzong Pang for serving as part of thesis committee. A special thanks to Dr. Krishna Krishnan, who guided me to the right path in the field of Computer Science. In addition, my thanks go to the Computer Architecture and Parallel Programming Laboratory (CAPP Lab), Department of Electrical Engineering and Computer Science and its staff for providing me the theoretical and practical knowledge in the courses in which I enrolled. Most importantly, I would also like to thank my parents, my sisters, and my friends for their help and support during my hardship and the completion of my goals.

ABSTRACT

The cloud computing environment has attained universal embrace in contemporary world. Its opulence is due predominantly to consumers' potential to use cloud amenities on demand with pay as you use protocol, which has validated being favorable. Despite of its evident merits, although, many enterprises hesitate to migrate from one cloud service provider to the other, primarily because of the issues associated to data migration, data lock-in, and security. In this work, we propose a cloud migration framework which addresses the data integrity issues, security and application lock-ins with the help of MySQL, tomcat server, java scripts, base concepts of amazon Database migration, Tsunami protocol, and cloud data logging framework in the cloud. We develop an enterprise specific migration framework to migrate the data from one cloud to the other cloud service once it is authorized by administrator. In case of any unauthorized user or service provider, the migration framework triggers an alarm message and locks the data using the cloud security framework integrated in migration framework. We simulate cases where migrations were successful and failed. Experimental results show that the time taken to migrate data is at least 20% less than the traditional data transfer, on an average size of the application and the bandwidth.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

Chapter Page

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES (continued)

LIST OF ABBREVIATIONS

API	Application Programming Interface
ETL	Extraction, Transformation and Loading
FAS	Fabric Attached Storage
Fsck	File utility system check
IaaS	Infrastructure as a Service
MBaaS	Mobile Backend as a Service
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random-Access Memory
NYT	New York Times
PaaS	Platform as a Service
SaaS	Software as a Service
SDK	Software Development Kit
SECaaS	Security as a Service
SLA	Service Level Agreement
WAFL	Write Anywhere File Layout

CHAPTER 1

INTRODUCTION

Cloud is a type of Internet related computing that delivers shared computer processing resources and data to systems and other devices on request [1]. It is a model for enabling universal, on-demand access to computer networks, servers, storage, applications and services, which can be quickly provisioned and released with nominal management effort [2][3]. Fundamentally, Cloud computing enables the users and enterprises with different capabilities to store and process their data in one of two privately owned cloud, or on a third-party server to enable data access easy and reliable. Data centers which are located far from the user–ranging in scope from across a area to across the world [4]. This type of computing relies on sharing of resources to attain flexibility and economy of scale, like the power grid over an electricity network.

Experts claim that cloud enables enterprises to avoid infrastructure costs (e.g., purchasing servers, storage media). Similarly, it enables organizations to concentrate on their core businesses instead of spending time and money on computer infrastructure [5]. Promoters also claim that cloud computing allows enterprises to get their applications running, with high efficiency and less maintenance, and enables information technology (IT) teams to quickly adjust resources to meet fluctuating and unpredictable business demand [5][6][7] . Cloud providers typically use a "pay as you go" model. This will lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model [8].

In 2009, the abundancy of high-capacity networks, low-priced computers and storage devices as well as the common use of hardware virtualization, service-oriented architecture, and autonomic and utility computing led to a rapid increase in migration to cloud computing [9]. Enterprises can scale up as computing needs increase and then scale down again as demands

decrease [10] [11]. In 2013, the survey results proved that the cloud computing had become a highly demanded service due to the advantages of high computing resources, low cost of cloud utilities, high performance, scalability, accessibility as well as availability [12]. Cloud service providers also experienced growth rates of 50% each year, but being still in a stage of early stages, it has pitfalls that need to be addressed to make cloud computing services more reliable and user friendly [13] [14] [15].

1.1 Evolution of the Cloud

The word cloud is usually used in science to represent a huge collection of objects that visually appear from a distance as a cloud and represents any set of things whose details are not further inspected in each context [16]. Another illustration of cloud is that the old scripts that sketched network schematics surrounded the icons for servers with a circle, and a collection of servers in a network remotely had several projecting circles, which represented a cloud [17]. The word cloud was used as a symbol for the Internet and a standardized cloud-like shape was used to denote a network on telephony schematics. Later it was used to depict the Internet in computer network diagrams. With this simplification, the implication is that the specifics of how the end points of a network are connected are not relevant for the purposes of understanding the diagram. The cloud symbol was used to represent networks of computing equipment in the original ARPANET by as early as 1977, [18] and the CSNET by 1981[19]—both predecessors to the Internet itself.

During the 1960s, the initial concepts of time-sharing became popularized via RJE (Remote Job Entry); this terminology was mostly associated with large vendors such as IBM and DEC [20]. Full time-sharing solutions were available by the early 1970s on such platforms as Multics (on GE hardware), Cambridge CTSS, and the earliest UNIX ports (on DEC hardware). The data center model in which users submitted jobs to operators to run on IBM mainframes was abundantly used.

During the 1990s, telecommunication companies began offering virtual private network (VPN) services with best quality of service, at a unique lower cost. By moving traffic as they seem related to balance server use, they could use whole internet bandwidth more efficiently. They started using the cloud symbol to represent the demarcation point between what the provider was accountable for and what users were accountable for. Cloud computing extended this boundary to range all servers as well as the network infrastructure [21]. As computers became more diffused, scientists and technologists explored ways to make large-scale computing power available to more users through time-sharing. They experimented with algorithms to optimize the infrastructure, platform, and applications to prioritize CPUs and increase efficiency for end users [22].

Since 2000, cloud computing has come into existence. During 2008, an open-source application for deploying clouds was developed by NASA named as OpenNebula, enhanced in the reservoir European Commission source funded project [23]. And, efforts were focused on providing quality of service guarantees to cloud-based infrastructures, in the framework of the IRMOS European Commission-funded project, yielding in a real-time cloud environment [24][25]. By mid-2008, Gartner saw an opportunity for cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them"[26] and observed that "organizations are switching from company-owned hardware and software assets to per-use service-based models" so that the "projected shift to computing will result in dramatic growth in IT products in some areas and significant reductions in other areas"[27].

Amazon introduced an Elastic Compute Cloud in August 2006 followed by announcement of Microsoft Azure as "Azure" in October 2008 and was released on 1 February 2010 as Windows Azure, before being named to Microsoft Azure on 25 March 2014. [29] In July 2010, Rackspace Hosting and NASA jointly launched an open-source cloud-software initiative known as

OpenStack. The early code initiated from NASA's Nebula platform and from Rackspace's Cloud Files platform. As an open source offering and along with other open-source solutions such as CloudStack, Ganeti and OpenNebula, it has attracted attention by several key communities. Several studies aim at comparing these open sources offerings based on a set of criteria [30] [31] [32] [33] [34] [35] [36].

On March 1, 2011, IBM declared the IBM SmartCloud framework to support Smarter Planet. [37] Among the various components of the Smarter Computing foundation, cloud computing is a critical part. On June 7, 2012, Oracle announced the Oracle Cloud. [38] While aspects of the Oracle Cloud are still in development, this cloud offering is poised to be the first to provide users with access to an integrated set of IT solutions, including the Applications (SaaS), Platform (PaaS), and Infrastructure (IaaS) layers [39] [40] [41].

In April of 2008, Google released Google App Engine in beta. In May of 2012, Google Compute Engine was released in preview, before being rolled out into General Availability in December of 2013 [42] [43].

Similar Concepts to Cloud Computing

The goal of cloud is to let users take advantage from all the below technologies, without the expertise with each one of them. The cloud mainly aims on cutting costs, and helps the users focus on their core business instead of being impeded by IT obstacles. [44] The main inspiring innovation for cloud computing is virtualizing resources and applications. Virtualization software distinguishes a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system–level virtualization creates a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Autonomic computing enables the

automation of the computing process through which the user can request or use resources on-demand. By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors [44]. Users routinely face difficult business problems. And cloud computing techniques use Service Oriented Architecture to break the problems into services and later are combined to provide a solution.

Cloud computing has similar characteristics with:

- Client–server model - Refers to any distributed application that distinguishes between service providers called as servers and service requestors also known as clients [45].
- Computer bureau - A service bureau providing computer services, particularly from the 1960s to 1980s.
- Grid computing - Distributed and parallel computing, in which a super and virtual machine is composed of a cluster of networked, loosely coupled computers behaving in sync to perform very large tasks.
- Green computing – Eco-friendly use of computing resources.
- Fog computing - Distributed computing paradigm that provides data, compute, storage and application services closer to near-user edge devices, such as network routers. Fog computing processes data at the network level, on smart devices and on the end-user client side, instead of sending data to a remote location for processing.
- Dew computing - Dew computing is positioned as the base for the cloud and fog computing paradigms. Dew computing pushes the frontiers to computing applications, data, and low-level services away from centralized virtual nodes to the end users [46].
- Mainframe computer - Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as: census; industry and consumer

statistics; police and secret intelligence services; enterprise resource planning; and financial transaction processing.

- Utility computing - The "packaging of computing resources, such as computation and storage, as a metered service like a traditional public utility, such as electricity"[47] [48].
- Peer-to-peer - A distributed architecture in which there is no need of central coordination. Peers or users are both suppliers and consumers of resources.
- Cloud sandbox - Cloud Sandbox is a live, private computer environment in which a program, code or file can run without affecting the application in which it runs.

1.2 Characteristics of Cloud

Using cloud over traditional storage has more benefits. An enterprise can save money, time and data with cloud computing. As shown in Figure 1 the cloud has some of the unique properties such as reduces infrastructure costs, increases capacity and scalability, easily refresh aging infrastructure, supports new business opportunities, helps in business continuity collaboration.

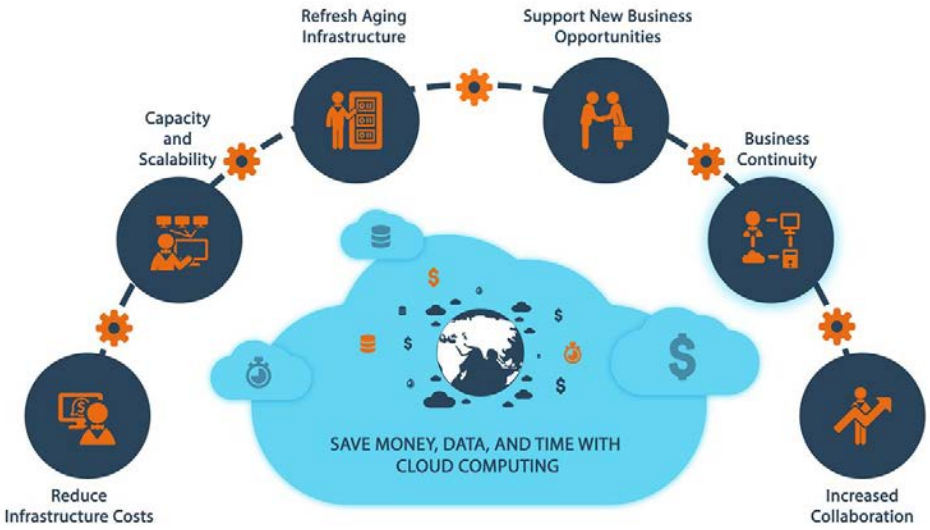


Figure 1. Merits of Cloud Computing

- Business for enterprises may be enhanced, as cloud computing may accelerate users' flexibility with re-provisioning, adding, or expanding technological infrastructure resources.
- Reductions in expenses are maintained by cloud service providers. A public-cloud delivery model converts primary expenditures (e.g., buying servers) to operational expenses [49]. This supposedly reduces barriers to entry, as infrastructure is typically provided by a third party and need not be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is "fine-grained", with usage-based billing options. As well, less in-house IT skills are required for implementation of projects that use cloud computing. [50] The e-FISCAL project's state-of-the-art repository contains several articles considering cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house [51].
- Device and location independence lets users to access systems using a web application or a browser regardless of their location or what device they operate (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect to it from any corner of the world [50] [52].
- Easy Maintenance of cloud applications due to its remote accessibility.
- Multi-tenancy enables sharing of resources and expenses across a vast group of users thus allowing for:
    - Shared infrastructure or central utilization in locations with lower costs (such as real estate, electricity, etc.)

    - Peak-load capacity increases (users need not engineer and pay for the resources and equipment to meet their highest possible load-levels)
    - Utilization and efficiency improvements for systems that are often only 10–20% utilized [53] [54].
- Performance is tracked by IT professionals from the cloud service provider, and consistent and loosely coupled architectures are constructed using web services as the system interface [50] [55] [56].
- Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their systems [57].
- Reliability increases with the adoption and use of multiple redundant sites, which makes well-structured cloud computing platform suitable for business continuity and disaster recovery [58].
- Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, OS and cloud providers [59] [60]), without users having to engineer for peak loads [61] [62] [63]. This gives the ability to scale up when the usage need increases or down if resources are not being used [64].
- Security can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is equally good or in some cases better than other traditional systems, in part because service providers can devote resources to solving

security issues that many customers cannot afford to tackle or which they lack the technical skills to address [65]. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

The National Institute of Standards and Technology's definition of cloud computing states five important characteristics of Cloud Computing:

- On-demand self-service: A user can use computing services when required automatically without any human intervention with each service provider.
- Broad network access: Capabilities are procurable over the network and usable through official mechanisms that endorse use by heterogeneous thin or thick client platforms such as mobile phones, tablets, laptops, and workstations.
- Resource Pooling: Cloud Service providers serve various customers or tenants with provisional and scalable services. These services can be modified to suit each client's needs without any changes being like the client or end user.
- Rapid Elasticity: Capabilities can be flexibly provisioned and released, in some cases self-regulating, to scale speedy inward and outward flexibility with demand. To the consumer, the capabilities available for provisioning often seem infinite and can be appropriated in any quantity at any point of time.
- Measured service: Services procured by the user can be reported, controlled, and monitored providing clarity for both the cloud provider and cloud consumer of the used service.

1.3 Cloud Service Models

Cloud-computing providers offer their "services" according to different models, of which the three standard models per National Institute of Standards and Technology are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [3]. These models offer increasing abstraction; they are thus often portrayed as a layer in a stack: infrastructure-, platform- and software-as-a-service, [68] but these need not be related. For instance, one can provide SaaS implemented on physical machines, without using underlying PaaS or IaaS layers, and conversely one can run a program on IaaS and access it directly, without wrapping it as SaaS. The NIST's definition of cloud computing defines the service models as follows [3]:

- Software as a Service (SaaS): The potential given to the user is to utilize the cloud service provider's applications running on a cloud platform. The cloud interfaces are accessible from different unique user devices a thin client interface, such as a email application, or a program interface. The cloud user does not monitor the underlying cloud platform including servers, operating systems, networks, storage, or even individual application abilities, except for limited user-specific application configuration settings.
- Platform as a Service (PaaS): The potential given to the client to convey onto the cloud storage made utilizing programming dialects, libraries, administrations, and devices bolstered by the cloud service provider. The consumer does not oversee or control the hidden cloud foundation including system, servers, working frameworks, or capacity, however has control over the conveyed applications and conceivably design settings for the application-facilitating condition.
- Infrastructure as a Service (IaaS): The capacity given to the cloud user is to arrange processing, storage, networks, and other essential processing assets where the user can

deploy and execute subjective programming, which can incorporate working infrastructure and applications. The cloud user does not oversee or control the hidden cloud infrastructure but rather has control over working operating systems, storage, and deployed applications.

IaaS, SaaS and PaaS

Cloud computing is classified into three services – Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) as shown in Figure 2. When a user can access cloud service through internet it is known as IaaS (Infrastructure as a Service). Internet based services such as storage and information bases are part of the IaaS which are consumed by the end users. We have other services named PaaS (Platform as a Service) and SaaS (Software as a service). PaaS can offer a full or incomplete application that users can admit and build on it; whereas SaaS provides a full application like ERP (Enterprise resource management) with the help of internet which is helpful in migrating to different infrastructure [69].

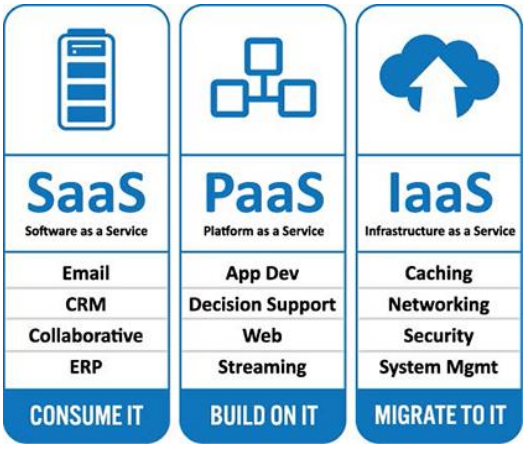


Figure 2. Outline of Services in Cloud Computing [71]

To get an idea of how IaaS work in real time scenario, consider how New York times had processed terabytes of data with the help of Elastic Compute Cloud (EC2) in the span of 36 hours otherwise it would have taken many months to process the data. The IaaS is separated into two

types of usage those are private and public. Amazon EC2 uses public server as the infrastructure in the cloud. A major private service cloud uses groups of public or private servers from an internal information center [70]. We can use both type of services to develop software inside the environment of the information center. The mixture of these services may provide latest updated applications which are known as hybrid clouds [71].

The IaaS is separated into two types of usage those are private and public. Amazon EC2 uses public server as the infrastructure in the cloud. A major private service cloud uses groups of public or private servers from an internal information center [70]. We can use both type of services to develop software inside the environment of the information center. The mixture of these services may provide latest updated applications which are known as hybrid clouds [71].

High end applications will be developed with the help of internet through Cloud computing. They extend their usability to the hardware as well as software. Users can access appliance themselves by not buying servers and upgraded software's. For the consumer, it is attainable through virtual resources. There is no limitation for its availability inside the venture, it can either be extensive software or hardware attained with the help of internet or both. The progress of enterprises will be varied to meet the above circumstances.

- SaaS: This type of cloud computing transmits programs through many clients via web browser. In this process user, can save a lot of expenses in the allocation of servers and software authorization.
- Utility Computing: This is an outdated thought. But it is used in Amazon, IBM and other major enterprises.

Cloud Computing has a close connection with SaaS, where the service providers use API's for developing applications not only on PC but also on internet. If it uses a middleman's device for

developing and delivering through servers & internet it is considered as platform for service. If a platform provides the interaction between users and providers such as budget management system managing budget and service providers is a mixture of SaaS and Management service provider known as Business service provider.

Infrastructure as a Service (IaaS) prioritizes services as- maximum priority for minimizing operating cost, migration to cloud, minimizing redundancies, helping startup companies move to cloud platforms, and supports inactive applications. Software as a Service (SaaS) gives maximum priority to minimize redundancies and helping startup companies to move to cloud. Platform as a Service (PaaS) gives maximum priority to Go-field development and migrating to cloud as shown in Table 1.

TABLE. 1

PRIORITIES IN VARIOUS SERVICES OF CLOUD

Priority	IaaS	SaaS	PaaS
Min Operation Costs	✓		
Go Field Development			✓
Migration to Cloud	✓		✓
Minimize Redundancies	✓	✓	
Startup Companies	✓	✓	
Inactive Applications	✓		✓

Three service Infrastructure used by various webs as being depicted in Figure 3 are as follows:

- Infrastructure as a Service in which full computer infrastructure such as storage and databases with the help of internet, is provided as a service to consumer or a system administrator [72].
- Platform as a Service provides partial application development such that user can access is specially used by developers.
- Software as a Service (SaaS) provides the entire Enterprise Resource Management through Internet to the end customers.

To understand better let us consider a scenario where New York Times wants to process terabytes of data using Amazon's EC2 instance within hours, if this was not a case if EC2 instance of Amazon is not used by NYT it would take months to process the terabytes of data through the cloud. This is taken care by Software as Service provider [73].

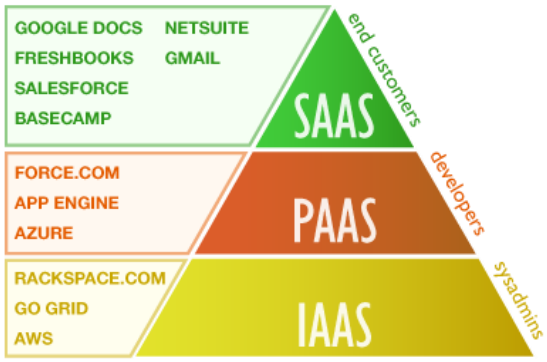


Figure 3. Various webs using the cloud services [74]

Security as a Service (SECaaS)

Security as a service (SECaaS) is a business model in which a large service provider combines their security services into an enterprise framework on a subscription basis more cost effectively

than most individuals or enterprises can provide on their own, when total cost of ownership is considered. In this situation, security is provided as a service from the cloud, without need of on-premises hardware preventing substantial capital outlays. These security services often include authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management, among others [74] [75].

Mobile Backend as a Service (MBaaS)

In the mobile "backend" as a service (m) model, also known as backend as a service (BaaS), web app and mobile app developers are provided with a way to link their applications to cloud storage and cloud computing services with application programming interfaces (APIs) exposed to their applications and custom software development kits (SDKs). Services include user management, push notifications, integration with social networking services and more [76]. This is a relatively recent model in cloud computing, with most BaaS startups dating from 2011 or later but trends indicate that these services are gaining significant mainstream traction with enterprise consumers [77] [78] [79] [80] [81].

Serverless Computing

Serverless computing is a cloud computing code execution model in which the cloud provider fully manages starting and stopping virtual machines as necessary to serve requests, and requests are billed by an abstract measure of the resources required to satisfy the request, rather than per virtual machine, per hour.[82] Despite the name, it does not actually involve running code without servers.[82] Serverless computing is so named because the business or person that owns the system does not have to purchase, rent or provision servers or virtual machines for the back-end code to run on.

1.4 Cloud Deployment Models

A cloud deployment model represents a specific type of cloud environment, primarily distinguished by ownership, size, and access.

There are four common cloud deployment models: [83]

- Public Clouds
- Community Clouds
- Private Clouds
- Hybrid Clouds
- Others (Virtual Private Cloud and Inter-Cloud)

Public Clouds

A public cloud is a publicly accessible cloud environment owned by a third-party cloud provider. The IT resources on public clouds are usually provisioned via the previously described cloud service models and are generally offered to cloud consumers at a cost or are commercialized via other avenues (such as advertisement). The cloud provider is responsible for the creation and on-going maintenance of the public cloud and its IT resources. Many of the scenarios and architectures explored in upcoming chapters involve public clouds and the relationship between the providers and consumers of IT resources via public clouds. Figure 4 shows a partial view of the public cloud landscape, highlighting some of the primary vendors in the marketplace.

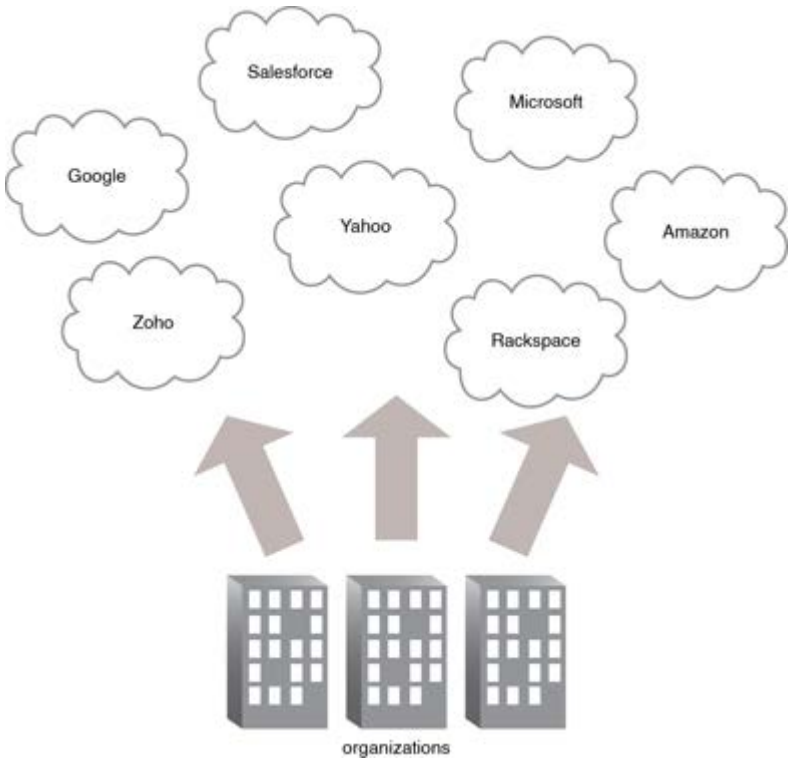


Figure 4. Organizations act as cloud consumers when accessing cloud services and IT resources made available by different cloud providers.

Community Clouds

A community cloud is like a public cloud except that its access is limited to a specific community of cloud users. The community cloud may be combined and owned by the community members or by a third-party cloud provider that provides a public cloud with restricted access. The member cloud users of the community typically share the responsibility for defining and evolving the community cloud. Membership in the community does not necessarily guarantee access to or control of all the cloud's IT resources. Users not belonging to the community are not granted access unless allowed by the community.

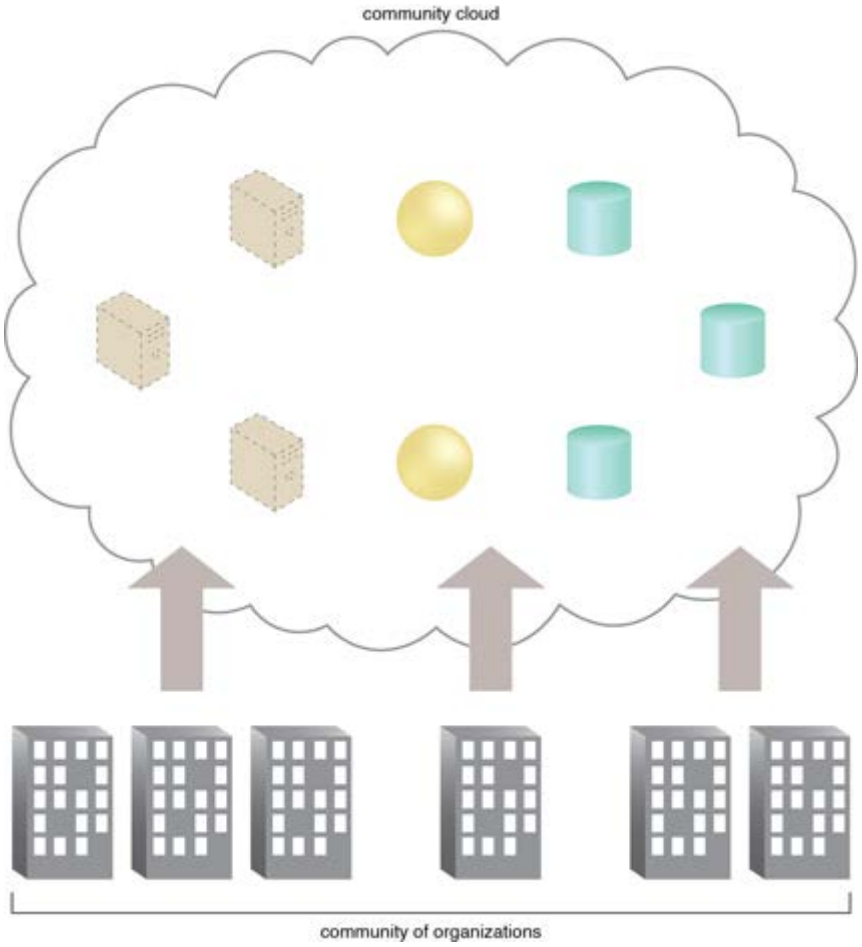


Figure 5. An example of a "community" of organizations accessing IT resources from a community cloud.

Private Clouds

A private cloud is accessed and used by a single enterprise. Private clouds lets an enterprise use cloud computing technology as a means of centralized access to IT resources by different parts, locations, or departments of the organization. When a private cloud performs as a controlled environment there are less issues involved. The use of a private cloud can change how organizational and trust boundaries are defined and applied and management is carried out by internal or outsourced staff.

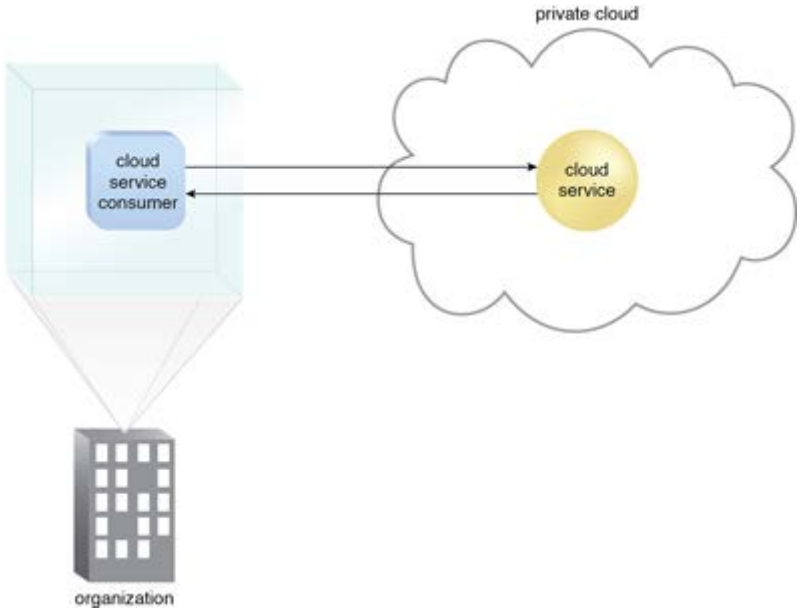


Figure 6. A cloud service consumer in the organization's on-premise environment accesses a cloud service hosted on the same organization's private cloud via a virtual private network.

Hybrid Clouds

A hybrid cloud is a cloud environment comprised of two or more different cloud deployment models. For example, a cloud consumer may choose to deploy cloud services processing sensitive data to a private cloud and other, less sensitive cloud services to a public cloud.

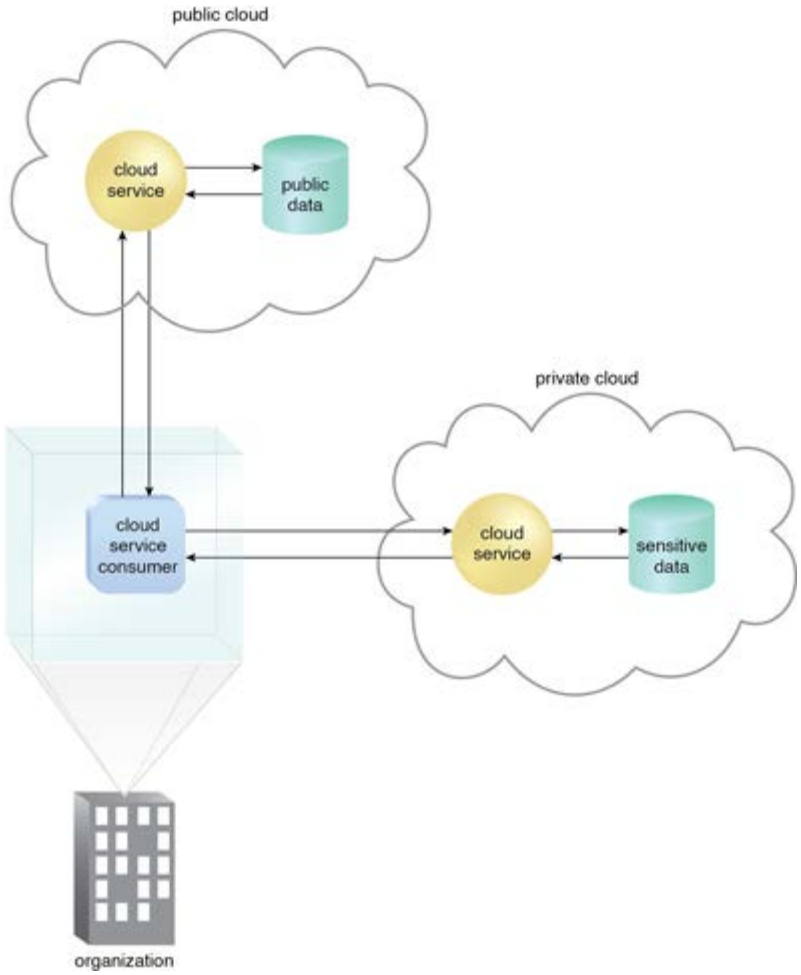


Figure 7. An organization using a hybrid cloud architecture that utilizes both a private and public cloud.

Others

Virtual Private Clouds - It is a self-contained cloud environment hosted and managed by a public cloud provider, and made available to a cloud user. Virtual private cloud is also called as dedicated cloud or hosted cloud.

Inter Clouds – Cloud architecture which involves more than one inter-connected clouds.

1.5 Primary Concerns in Cloud Computing

Concern about security and privacy in the cloud will drive adoption of cloud encryption systems, but the survey warns there are security issues that businesses should tackle. The expected compound annual growth rate of software as a service (SaaS) from 2011 to 2016 is 19.5%, platform as a service (PaaS) 27.7%, infrastructure as a service (IaaS) 41.3% and security services spending 22%.

However, security and privacy are still cited by many organizations as the top inhibitors of cloud services adoption, which has led to the introduction of cloud encryption systems in the past 18 months. While encryption is important to the secure adoption of cloud services, it should not be viewed as the "silver bullet". Analysts recommend that enterprises should first develop a data security plan that addresses five security issues. Failure to do so, they say, could add cost and complexity to the adoption of cloud computing without addressing the fundamental issues of data privacy and long-term security and resiliency. They warn that badly implemented encryption systems may also even interfere with the normal functioning of some cloud-based services.

The issues that must be addressed are:

- Breach notification and data residency
- Data management at rest
- Data protection in motion
- Encryption key authority
- Access controls

Breach Notification and Data Residency

Not all data requires equal protection, so businesses should categorize data intended for cloud storage and identify any compliance requirements in relation to data breach notification or if data may not be stored in other jurisdictions. Analysts also recommend that enterprises should put in place an enterprise data security plan that sets out the business process for managing access requests from government law enforcement authorities. The plan should take stakeholders into account, such as legal contracts, business units, security and IT.

Data Management at rest

Businesses should ask specific questions to determine the cloud service provider's (CSP's) data storage life cycle and security policy.

Businesses should find out if:

- Multi-tenant storage is being used, and if it is, find out what separation mechanism is being used between tenants.
- Mechanisms such as tagging are used to prevent data being replicated to specific countries or regions.
- Storage used for archive and backup is encrypted and if the key management strategy includes a strong identity and access management policy to restrict access within certain jurisdictions.
- Data Analysts recommend that businesses use encryption to implement end-of-life strategies by deleting the keys to digitally shred the data, while ensuring that keys are not compromised or replicated.

Data Protection in Motion

As a minimum requirement, analysts recommend that businesses ensure that the CSP will support secure communication protocols such as SSL/TLS for browser access or VPN-based connections for system access for protected access to their services. The research note says that businesses always encrypt sensitive data in motion to the cloud, but if data is not encrypted while in use or storage, it will be incumbent on the enterprise to mitigate against data breaches. In IaaS, the businesses favor CSPs that provide network separation among tenants, so that one tenant cannot see other's network traffic.

Encryption key authority

Enterprises should always aim to manage the encryption keys, but if they are managed by a cloud encryption provider, they must ensure access management controls are in such a place that will satisfy breach notification requirements and data residency. If keys are managed by the CSP, then businesses should require hardware-based key management systems within a tightly defined and managed set of key management processes. When keys are managed or available in the cloud, it is imperative that the vendor provides tight control and monitoring of potential snapshots of live workloads to prevent the risk of analyzing the memory contents to obtain the key.

Access Control

The Enterprises require the CSP to support IP subnet access restriction policies so that they can restrict end-user access from known ranges of IP addresses and devices. The enterprise should demand the encryption provider to offer adequate user access and administrative controls, stronger authentication alternatives such as two-factor authentication, management of access permissions, and separation of administrative duties such as security, network and maintenance.

Businesses should also require:

- Logging of all user and administrator access to cloud resources, and provide these logs to the enterprise in a format suitable for log management or security information and event management systems.
- The CSP to restrict access to sensitive system management tools that might "snapshot" a live workload, perform data migration, or back up and recover data.
- That images captured by migration or snapshotting tools are treated with the same security as other sensitive enterprise data.

1.6 Motivation

Hybrid Cloud Vs Private Cloud

In 2017, since the last State of the Cloud Survey, it was observed that private cloud adoption fell slightly. The percent of respondents now adopting private cloud is 72%, down by 5% that is 77% last year. As a result, use of hybrid cloud environments has degraded to 67% from 71% last year. In total, 95% of respondents are now using cloud as shown in Figure 8 [84].

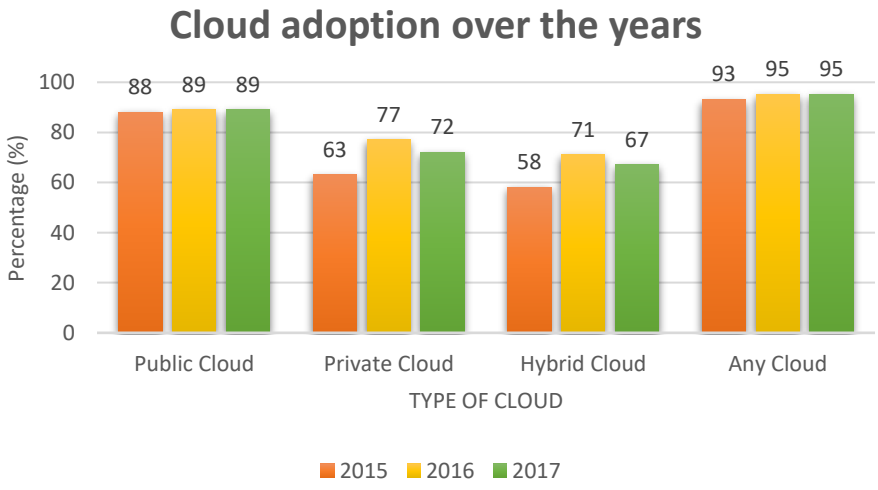


Figure 8. Statistics showing the adoption of cloud 2015-2017 [84].

The percentage of enterprises that have a plan to use multiple clouds increased to 85% (compared to 82% in 2016) with 58% planning on hybrid (55% in 2016). There was also an great increase in the number of enterprises planning for multiple public clouds (up from 16% to 20%) and a concurrent decrease in those planning for multiple private clouds (down from 11% to 7%) shown in Figure 9 [84].

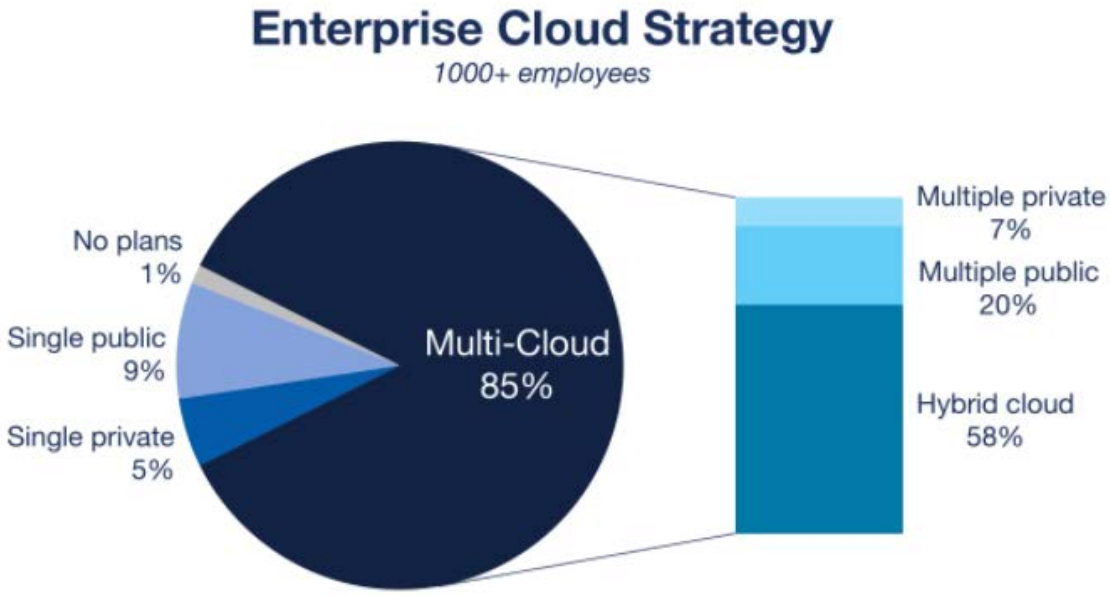


Figure 9. Enterprises Planning on adopting Cloud Technologies [84].

Cloud users running applications using Multiple Clouds

Companies that use public cloud are already running applications in an average of 1.7 public clouds and experimenting with another 1.7 public clouds. While fewer companies are using private clouds, those that do use more, running applications in an average of 2.4 private clouds and experimenting with an additional 2.2 private clouds as indicated in Table 2 out of index 5.0 [84].

TABLE. 2

CLOUD USERS RUNNING APPLICATIONS ON MULTIPLE CLOUDS OUT OF INDEX 5.0 [84]

No of Clouds used	Public Cloud Users	Private Cloud Users
Running Applications	1.7	2.4
Experimenting	1.7	2.2
Total	3.4	4.6

Enterprises run majority of workload in Clouds

Companies now run 79% of workloads in cloud, with 41% of workloads in public cloud and 38% in private cloud. It's important to note that the workloads running in private cloud may include workloads running in existing virtualized environments or bare-metal environments that have been cloudified as illustrated in Figure 10 [84].

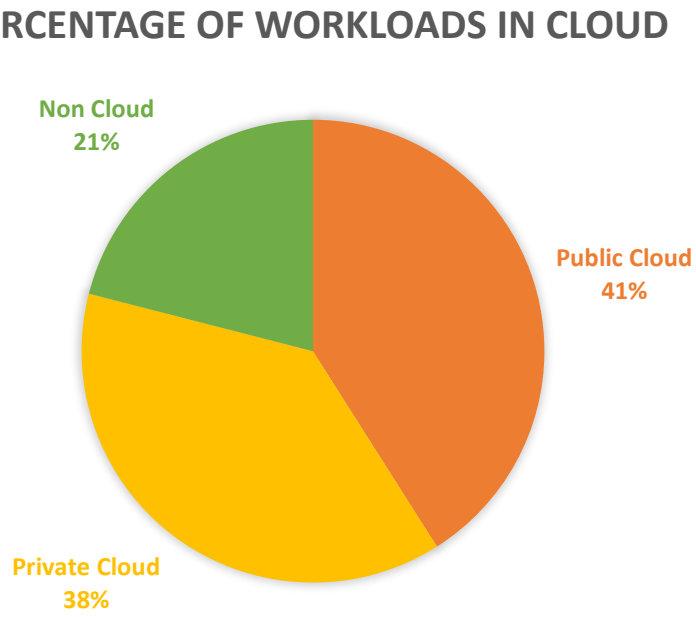


Figure 10. Percentage of Workload in Clouds [84].

Enterprises run 75% of workloads in cloud with more in private cloud (43%) vs. public cloud (32%). Small and Medium Sized Businesses run 83% of workloads in cloud with more in public cloud (50%) vs. private cloud (33%) as represented in Figure 11 [84].

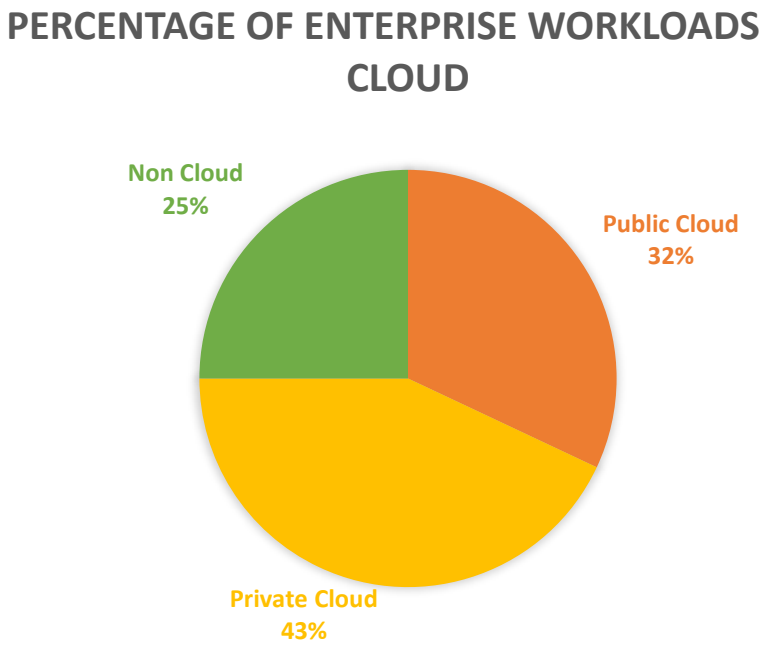


Figure 11. Percentage of Enterprise Workloads in Cloud [84].

Enterprise IT Teams take a strong cloud role

According to RightScale report 2017, it states that they saw a strong shift toward centralization, with more central IT teams taking a broader view of their role in cloud. They see a role for themselves in selecting public clouds (65%), deciding/advising on which apps to move to cloud (63%), and selecting private clouds (63%) shown in Fig 12 [84].

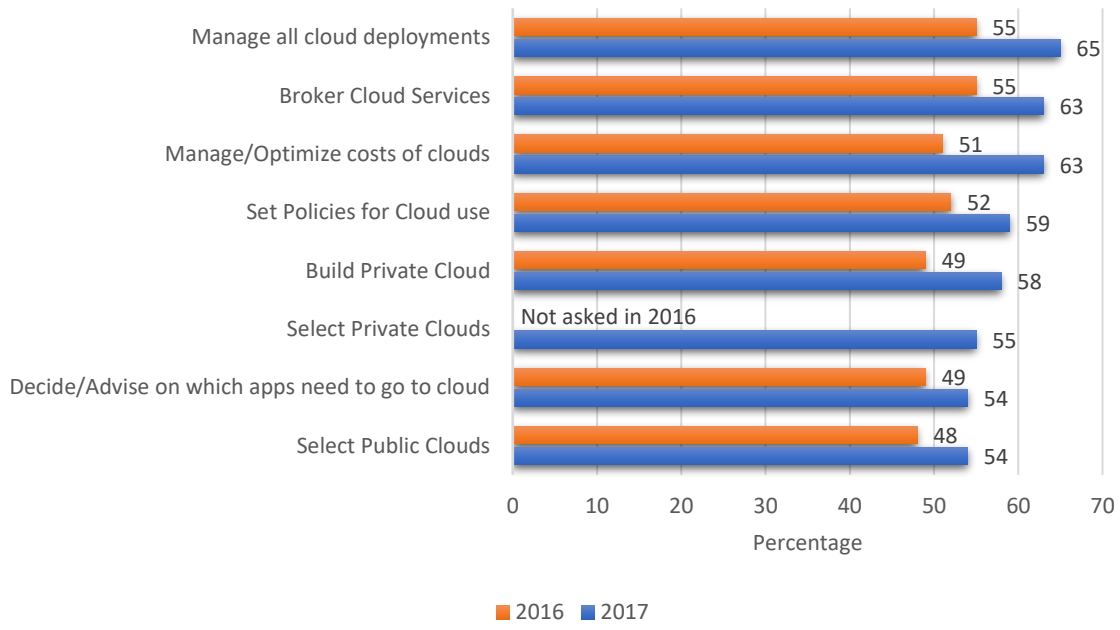


Figure 12. Enterprise Central IT View of role [84].

Cloud Challenges decline overall: Expertise, Security and expenses for #1

In 2017, expertise, security, and spend were all compared for the top challenge with 25% of cloud users citing each as a significant challenge. Lack of resources/expertise, cloud challenge in 2016, was less of a challenge in 2017 with only 25% mentioning it as a major concern, down significantly from 32% in 2016. Concerns about security fell to 25% vs. 29% last year. Administrating cloud expenses fell only slightly from 26% to 25% as shown in Figure 13 [84].

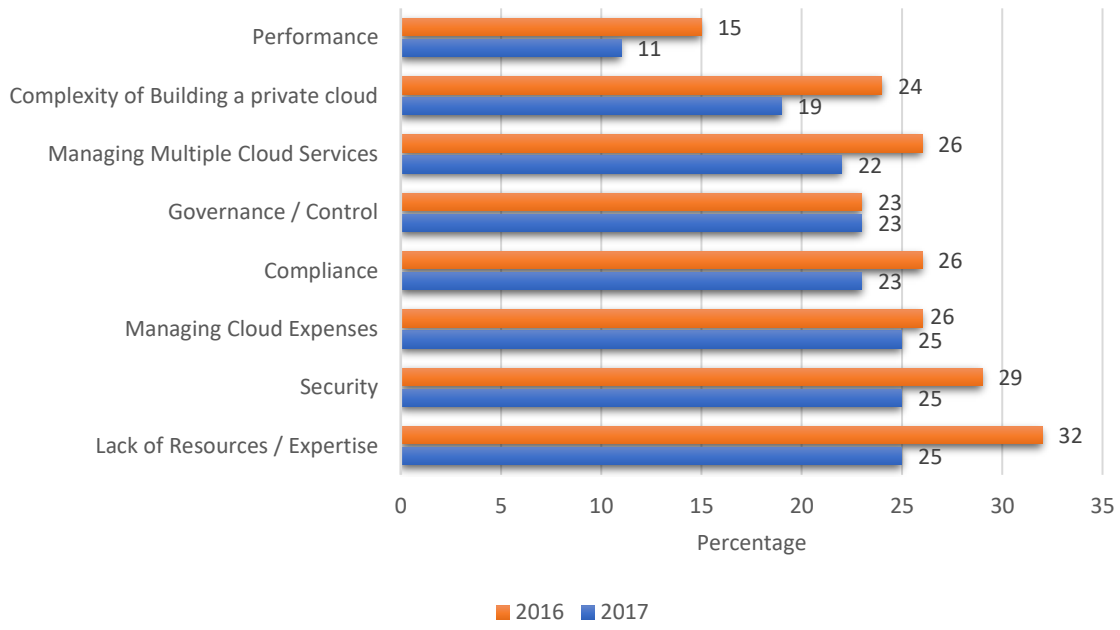


Figure 13. Cloud Challenges 2016 vs. 2017 [84].

Wasted Cloud Spend a major challenge for reducing costs

Even as managing cloud expenses emerges to be a major challenge, cloud users ignore the amount of wasted cloud spend. Cloud Users estimate 30% waste, while RightScale has measured actual waste between 30% and 45% [84].

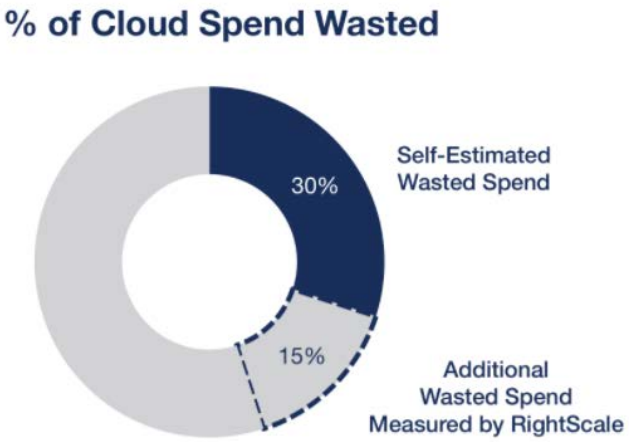


Fig. 14. Percentage of Cloud spend wasted according to RightScale Report 2017 [84].

This raised concern about costs has made optimizing cloud costs the top initiative and challenge for 2017 across all cloud users (53%) and especially in mature cloud users (64%) as shown in Figure 15.

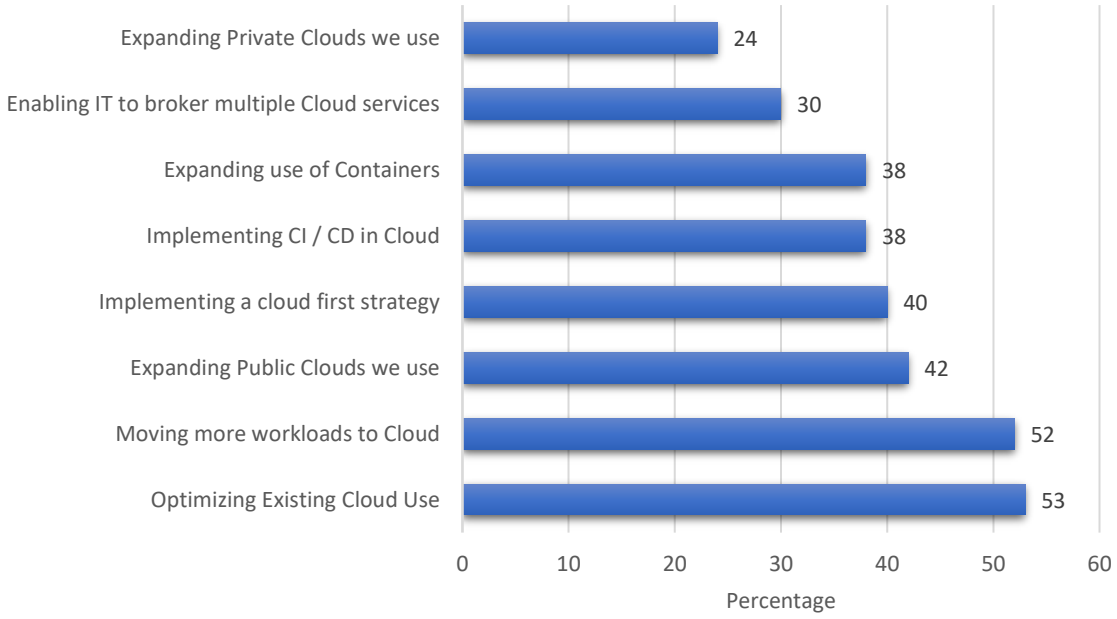


Figure 15. Cloud Initiatives in 2017 [84].

When many enterprises tend to move towards using Cloud Technologies, we at Wichita State University think that there could be some contribution made towards cloud computing enabling enterprises to move data from one cloud to other cloud easier. This above statistics and emerging use of cloud motivates us to start a contributing work towards cloud computing.

1.7 Problem Description and Contribution

Despite simplicity being one of the major strengths for Cloud computing; at last it is one of its loopholes. For private purpose, the intricacy is relatively negligible and moving from cloud vendor to another is difficult due to its simplicity and the security.

When enterprise has a large data to be migrated from Storage center to Cloud, they rarely worry about issues like application compatibility, security and data integrity because they own their storage devices. In the same manner, when the data is migrated to a cloud and the enterprise is not satisfied with the service provider, they can't migrate their data easily because factors like application compatibility, security, cost and data integrity effects the migration and they end up spending more than what is needed on unsatisfied cloud service. When we think of data transfer from cloud to cloud it seems to be like network to network data transfer (considered to be easy as it used dedicated resource), but it is difficult to maintain security in shared resource like cloud. And hence we are trying to resolve the Security, Migration and Data Integrity issues in this work.

We propose a new framework which enables enterprises to migrate data of any size without worrying about the application compatibility, security and cost using the Amazon Tsunami Protocol, Java Scripts, and NetApp NVRAM (Non-Volatile Random-Access Memory) and WAFL (Write Anywhere File Layout). Our framework, secures the enterprises' data, enables data migration from one cloud to another (enterprise choice of choosing new cloud service provider) and reduce the overall cost to handle data as the framework is platform independent and needs less user intervention.

1.8 Thesis Organization

This thesis manuscript is organized as follows:

- In Chapter 2, we discuss in detail about the Problem Description, Migration Methodologies, Issues faced in Cloud Migration and all-important terms and techniques used in Cloud Migration framework.
- In Chapter 3, we introduce the proposed Cloud Migration framework. We also discuss the workflow and algorithms of the proposed methodology comprehensively.
- In Chapter 4, we describe experimental setup details, which are considered in this research.
- In Chapter 5, we illustrate some experimental results to evaluate the proposed methodology.
- In Chapter 6, we conclude this research and list some possible future scopes of research in this field.
- Finally, in Chapter 7 we list all the references which were used in framing this framework.

CHAPTER 2

LITERATURE SURVEY

In this chapter, we discuss the theoretical concepts of Cloud Computing, Types of Migration, Issues in Cloud Migration, Migration Methodologies, Data Logging Security framework related information that has been considered in this research.

Migration is termed as moving the data from source to destination. Migration requires the host machine coordinates the relocation of the files as shown in Figure 16 from source to destination through relocation scheme. We had to set up a move without trailing the partition of apprehension between the management and implementation or a backup, while still sticking to the essentials such as security, scalability and efficiency.

Figure 16. Migration of Data from Source to Destination.

2.1 Types of Migration

Data Migration

The method of transferring data of different formats between storage drives or computers is referred as data migration. To achieve an automated migration, it must be done programmatically.

PC Migration

The process of changing the whole environment for the user is considered as Personal Computer migration (PC migration). It deals with the concept of total cost of ownership where the requirement to migrate data is decided upon a "cost" in buying a new PC.

Process Migration

It is processed mainly in the clusters of computers, where there is a possibility to move a process from one machine to the other. Its alternate is from IC design and engineering. It is a design flow to change and shrink an existing layout to a new process node. It could be manually checked with the help of automatic CAD tools.

System Migration

It mainly deals with a set of programs from one platform to another. It involves a down time while the old is replaced with a new one.

2.2 Migration Methodologies

To understand how the data is migrated in the cloud the following scenarios of migration in wall phones, cell phones, changing the Personal Bank Account to another Bank, Migration in Database and Migration in Cloud gives us a crystal-clear view:

Migrating Career in Wall / Cell Phone

Wall phone number portability allows customers to change their respective service from one company to a new one exclusive of changing their number. To migrate from one wall phone carrier to another wall phone carrier it should follow the following steps as shown in Figure 17.

- *Step 1:* Select a carrier that you wish to migrate to and make your obligation based on plan options and coverage. Choose the carrier based on the needs of your family or business.
- *Step 2:* Call the new wall phone carrier and confirm whether you are eligible for migrating the phone carrier.
- *Step 3:* Order the switch for the new wall phone carrier you opted for. The new carrier will handle the transfer process. Moving a switch from one carrier to another carrier might take few hours.
- *Step 4:* Keep our old wall phone carrier until the old service is deactivated. We can continue to handle our old wall phone till we have the switch. [85]

Figure 17. Steps Involved in migration of wall phone carrier & Cellular phone.

Changing Personal Bank Account

When any Bank charges more unnecessary fees and charges, the banker or the customer gets frustrated. When the customers are not satisfied with their current Bank, they try to migrate or change the Bank of their choice. When the customers close their old Bank account, they make

sure that no personal details and sensitive information such as Social Security Number, Name, Address and other important information is sustained with the old bank. Following are the steps involved in migrating the bank account from one bank to another.

- *Step 1:* Find a new Bank, which the customer is happy with and satisfied.
- *Step 2:* Open a new Account with the new Bank.
- *Step 3:* Transfer all the cash and balance from old bank account to the new one.
- *Step 4:* Switch over all payments such as Direct Deposits and bill payments.
- *Step 5:* Close the old bank account and shred all the important information related to the old bank account.
- *Step 6:* Make sure that the old bank does not hold your sensitive information to prevent identity theft and identity ware.

Migration in Database

The database migration is also known as schema migration which refers to the management of incremental, reversible alterations to relational. A database migration is performed on a database whenever it is necessary to update or revert that database's schema to some newer or older version. Database Migrations are accomplished programmatically by using a database migration tool. When invoked with a specified desired schema variant, the migration application automates the consecutive application or setback of a proper order of schema changes until it is brought to the desired state.

Many database migration applications aim to shrink the effect of schema changes on any existing data in the database. In contempt of this, maintenance of data in common is not assured because schema changes such as the deletion of a database column can damage data (i.e. all values entered in that column for all rows in that table are deleted). Rather, the tools aid to maintain the

definition of the data or to reorganize existing data to meet new requirements. After all the meaning of the data usually cannot be encoded, the configuration of the tools usually needs manual intervention [86].

The process of database or schema migration begins with the source database Extraction, transformation and loading (ETL) with ad-hoc analysis as shown in Figure 18. After the ETL process multiple iterations of data are tested to see whether is there any data which is platform dependent. If there is any table which is platform dependent, it is transformed such that it is platform independent. Further, using the database migration tools like Flyway, LiquiBase, or any other tools. Then there is a chart which represents the factors that matter in migration process like the datatypes, the Operating system of the database and it is compared to the target database. If there are no issues, then the customer chooses the new platform from the list available and the data is successfully migrated without any complexities.

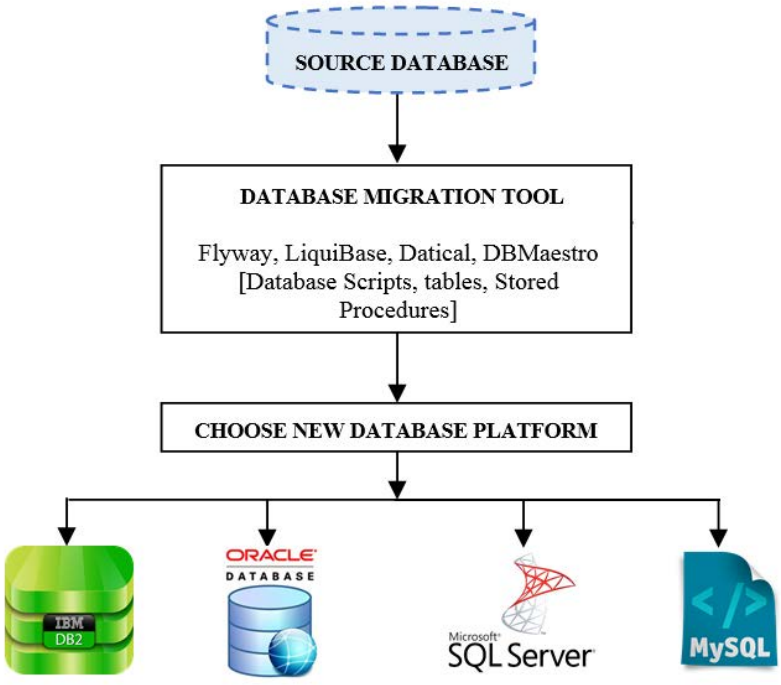


Figure 18. Database/Schema Migration Process.

2.3 Migration in cloud and Challenges in Cloud Migration

The major challenge in the cloud migration technology or framework is we need to make sure that large amounts of data should move far and fast. Cloud migration is classified in to following:

- Migration from data centers to cloud: Here the data will be migrated with the help of data centers. At first the source will send the data into datacenters, where these will take care of the successful migration.
- Cloud to Cloud data migration: Here the data can be moved from one cloud to another cloud (as shown in Figure 19). This process is known as cloud migration.

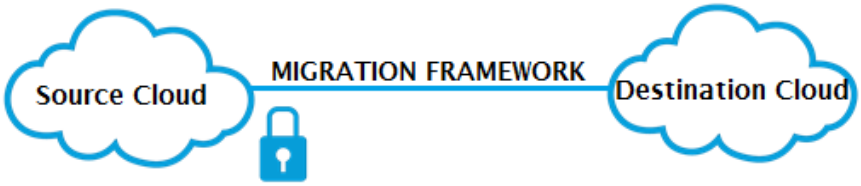
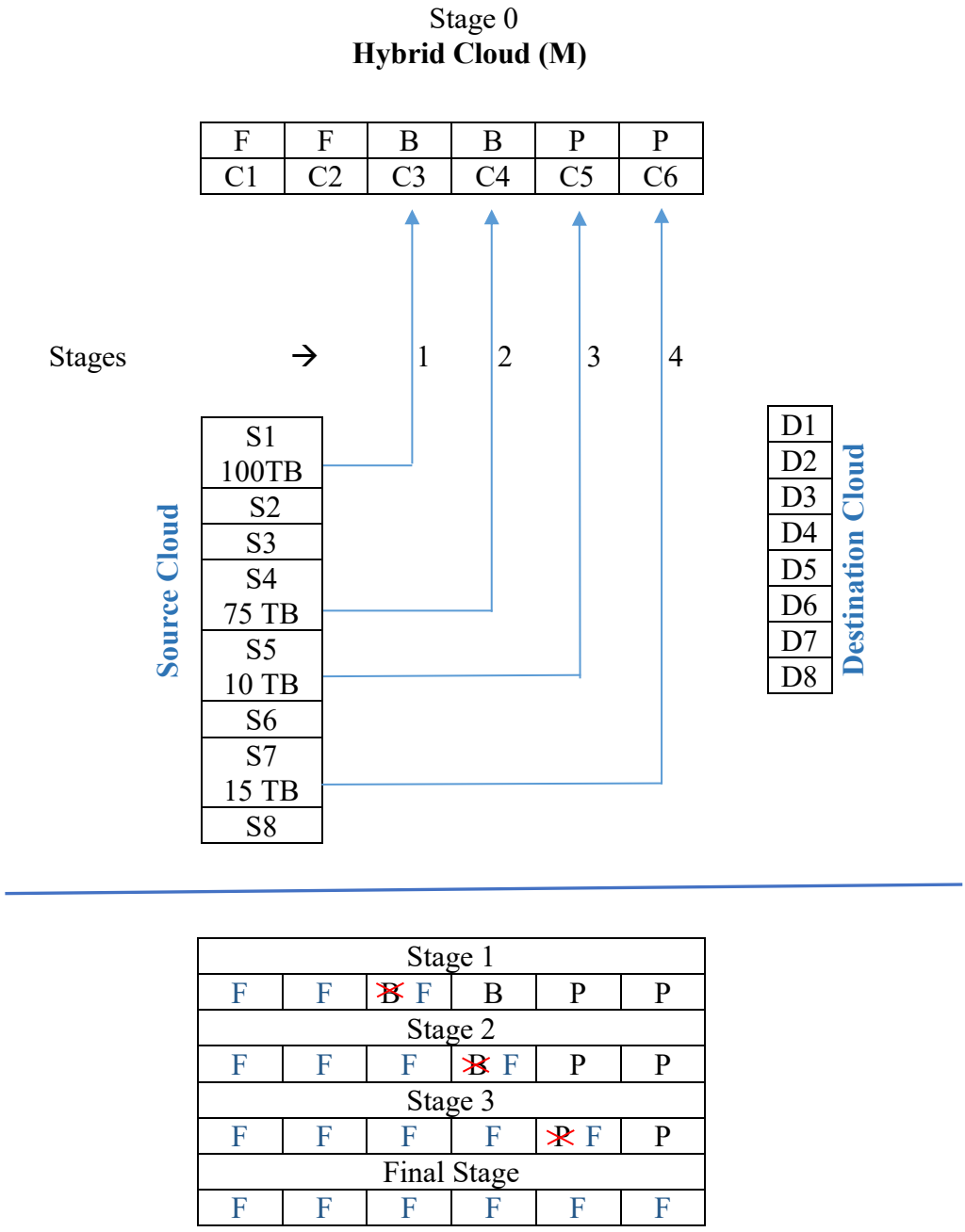


Figure 19. Cloud to Cloud data Migration Base Framework.

We move from one cloud to another because of the following factors such as better cost [87], improved services, better management and security. Generally, cloud to cloud migration is a complex process. This paper offers the best solution for the cloud to cloud issues [72].

In this research, we propose a framework for the migration of cloud from one service provider to the other mainly for the enterprise applications. In common, many enterprises have cloud storage which runs their application on it, so if there is any issue with the present cloud service the enterprise is using the enterprise is in a dead lock situation. Some issues that an enterprise face is sudden increase of cost of cloud, Service Level Agreement issues, lack of service, data security, and cloud restorability time.



Where, F – Filled
P – Partially filled
B – Blank or Empty

Figure 20. Migration of data between different clouds of Single Enterprise.

The Cloud storage in large enterprises handles huge amount of secured data, enterprise may not feel comfortable to migrate the data. Even if there is a misunderstanding with a single vendor with other vendors, this might be considered a serious issue. Here the data might be corrupted because a huge amount of data will be accumulated in the cloud. e.g. “5 Mb/second bandwidths 95% of the time overlaps with some other time”, due to this “no more than certain number of concurrent cloud users at any time” [88]. A scenario of issues in migration is discussed in Figure 20.

We consider ‘S’ to be a collection of various sources such as (S1,S2,S3….S8), where ‘D’ is considered to be a collection of various ending points such as (D1,D2,D3,….Dn), M (Hybrid cloud) is considered to be the combination of various clouds such as (C1,C2,C3…Cn) , F is considered to be a cloud in completely filled or busy state, P is considered to be partially filled and B is considered to be cloud is in free or blank (Note : in federated clouds various clouds are the combination of clouds from different vendors). Stage 0 is initial state (original state) of the federated clouds as shown in the fig 8. In stage1 S1 has 100 Tb of data which is tried to move its data to C3 because it has empty or null space inside it. When the data is migrated to cloud C3, B will be changed to F state. In stage 2 S4 has 75 Tb of data where it tries to move its data to C4 because its storage capacity is empty. When the data is migrated to cloud C4, B will be changed to F state. In stage 3 S5 has 10 Tb of data, where it tries to move its data to C5 because it is partially filled, and it can be utilized. When the data is migrated to cloud C5, P will be changed to F state. In stage 4 S7 has 15 Tb of data, where it tries to move its data to C6 because its storage capacity is partially filled. When the data is migrated to cloud C6, P will be changed to F state. In the final stage when it reaches the completed F then there will be a problem. It may not be able to operate the databases and the result of this leads to decrease in its band width. Time might also be an issue, because it takes lot of time to migrate from one cloud to other. It is very hard to resolve the security issues.

2.4 Backbone of this Framework

2.4.1 Amazon Web Services Cloud Migration Framework

The amazon web services cloud migration framework and the hardware support the migration of data from the traditional storage devices to the cloud. The main components in this technology are Direct Connect (Separate S3 and EC2 so that it maintains separation between environments), Snowball (provides high level security while transferring data to the cloud and faster transfer), Storage Gateway (links the enterprises environment to the cloud infrastructure and lets the enterprise build a hybrid cloud very easily) and some S3 connectors with leading software packages for the data backup, visibility and control over the data catalog.

In the procedure shown in Figure 21, the database copy is transferred to an Amazon EC2 instance and the data is imported into a new Amazon database instance. Then the replication process is used to bring the Amazon database instance up-to-date with your live external instance, before redirecting the application to the database instance. Configure Maria database replication depending on global transaction identifiers and check for the compatibility versions. If not compatible configure replication based on binary log coordinates.

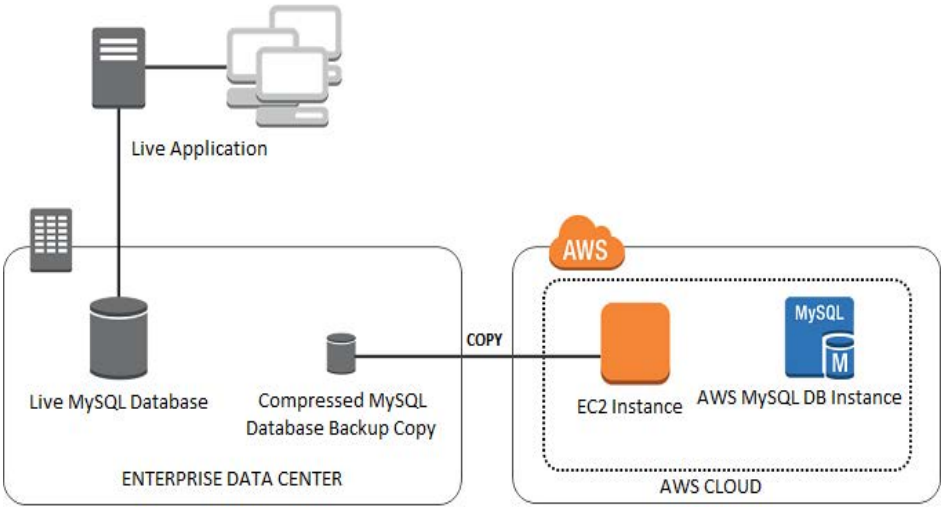


Figure 21. Amazon Cloud Migration Replication Process.

2.4.2 Write Anywhere File Layout (WAFL) and NVRAM

The Write Anywhere File Layout (WAFL) is a file layout that supports large, high-performance RAID arrays, quick restarts without lengthy consistency checks in the event of a crash or power failure, and growing the filesystems size quickly. It was designed by NetApp for use in its storage appliances.

WAFL is a UNIX compatible file system optimized for network file access. In many ways WAFL is like other UNIX file systems such as the Berkeley Fast File System (FFS) [McKusick84] and TransArc's Episode file system [Chutani92]. WAFL is a block-based file system that uses Inodes to describe files. It uses 4 KB blocks with no fragments. Each WAFL Inodes contains 16 block pointers to indicate which blocks belong to the file. Unlike FFS, all the block pointers in a WAFL inode refer to blocks at the same level. Thus, inodes for files smaller than 64 KB use the 16 block pointers to point to data blocks.

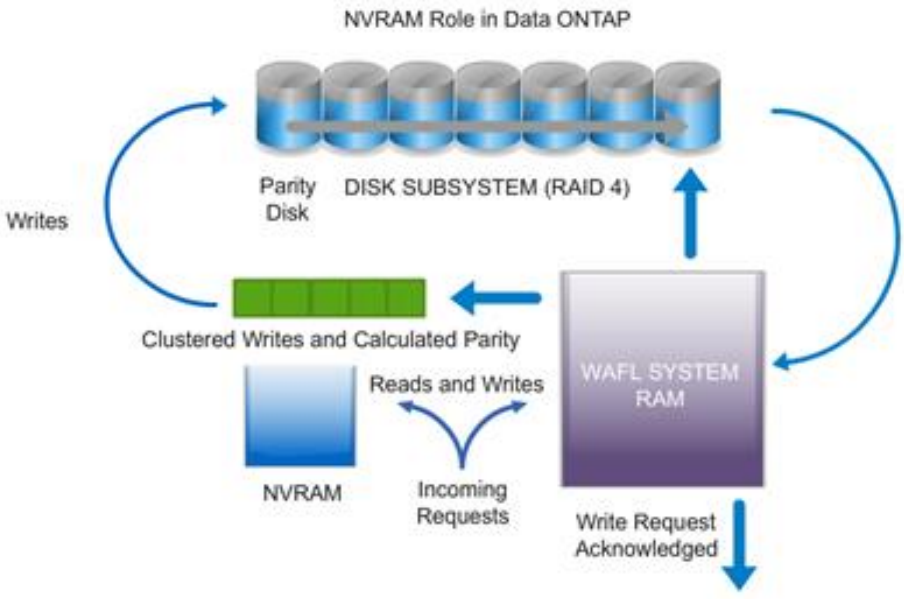


Figure 22. How NVRAM and WAFL work

Inodes for files smaller than 64 MB point to indirect blocks which point to actual file data. Inodes for larger files point to doubly indirect blocks. For very small files, data is stored in the inode itself in place of the block pointers as shown in Figure 22.

WAFL overcomes the classic parity-disk hotspot issue, using flexible write allocation policies:

- Writes any filesystem block to any disk location (data and meta data)
- New data does not overwrite old data
- Assigns disk space for many client-write operations at once in a single new RAID-stripe write (no parity re-calculations)
- Writes to stripes that are near each other
- Writes blocks to disk in any order

Like Episode, WAFL stores meta-data in files. WAFL's three meta-data files are the inode file, which contains the inodes for the file system, the block-map file, which identifies free blocks, and the inode-map file, which identifies free inodes. The term *map* is used instead of *bit map* because these files use more than one bit for each entry. The block-map file's format is described in detail below in Fig 23 (a).

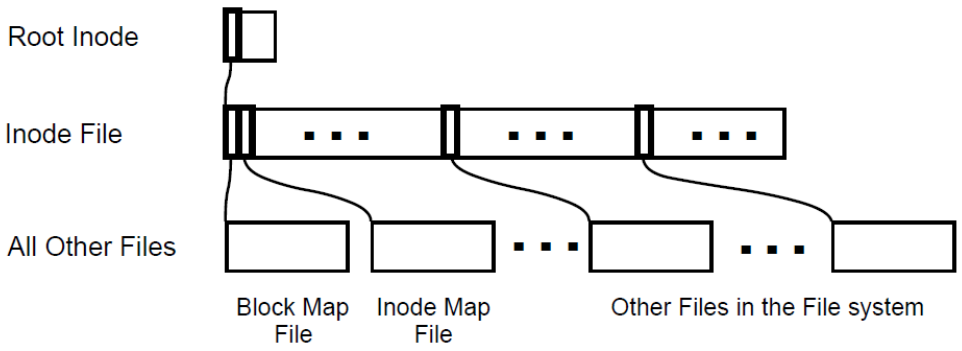


Figure 23 (a). The WAFL file system

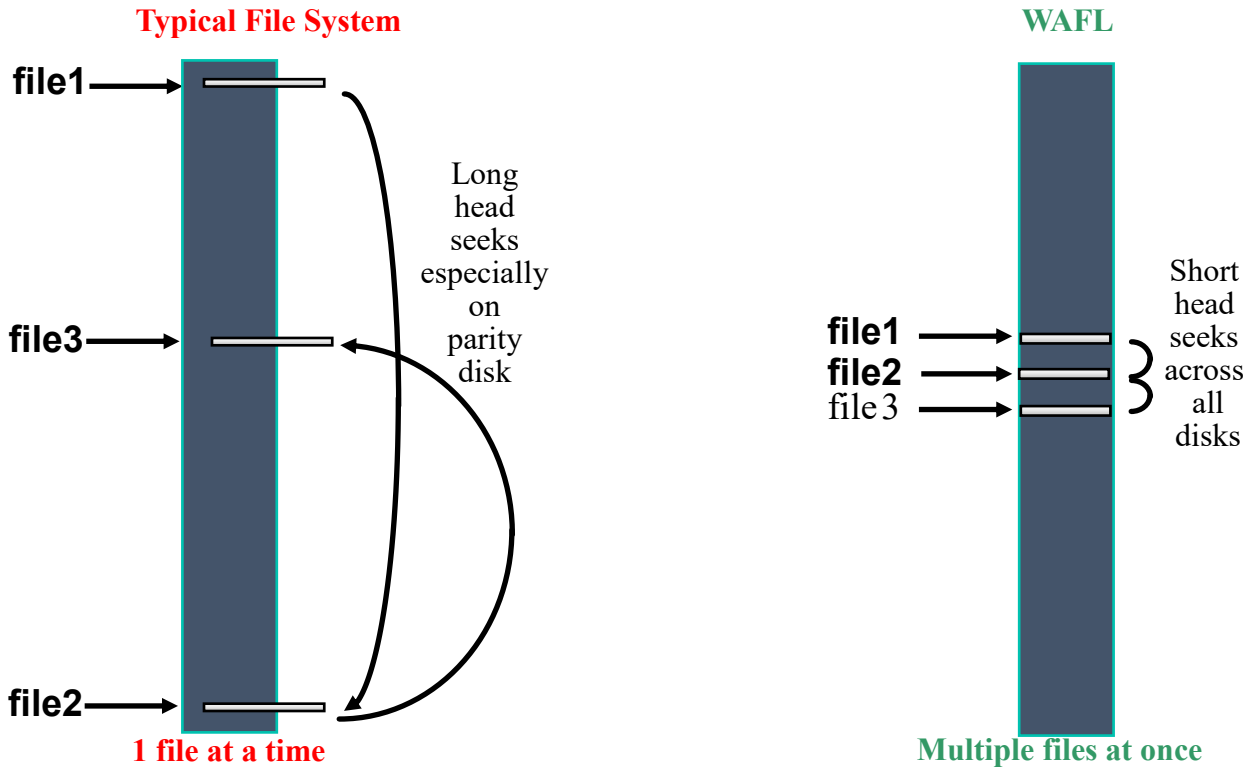


Figure 23 (b). The WAFL file system which describes the inode file, at the top, and meta-data files and regular files underneath.

Keeping meta-data in files allows WAFL to write meta-data blocks anywhere on disk. This is the origin of the name WAFL, which stands for Write Anywhere File Layout. The write-anywhere design allows WAFL to operate efficiently with RAID by scheduling multiple writes to the same RAID stripe whenever possible to avoid the 4-to-1 write penalty that RAID incurs when it updates just one block in a stripe. Keeping meta-data in files makes it easy to increase the size of the file system on the fly. When a new disk is added, the Fabric Attached Server automatically increases the sizes of the meta-data files. The system administrator can increase the number of inodes in the file system manually if the default is too small. Finally, the write-anywhere design enables the copy-on-write technique used by Snapshots. For Snapshots to work, WAFL must be able to write

all new data, including meta-data, to new locations on disk, instead of overwriting the old data. If WAFL stored meta-data at fixed locations on disk, this would not be possible.

A WAFL file system is best thought of as a tree of blocks. At the root of the tree is the root inode, as shown in Figure 23 (b). The root inode is a special inode that describes the inode file. The inode file contains the inodes that describe the rest of the files in the file system, including the block-map and inode-map files. The leaves in the tree are the data blocks of all the files. Figure 24 is a more detailed version of Figure 23 (b). It shows that files are made up of individual blocks and that large files have additional layers of indirection between the inode and the actual data blocks. For WAFL to boot, it must be able to find the root of this tree, so the one exception to WAFL's write-anywhere rule is that the block containing the root inode must live at a fixed location on disk where WAFL can find it.

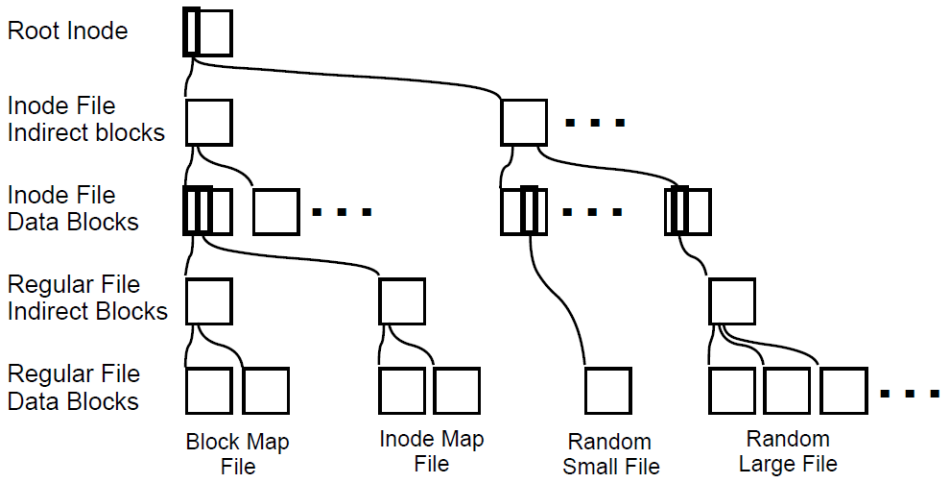


Figure 24. Detailed view of WAFL's tree of blocks

WAFL neglects the need for file system consistency checking after an improper shutdown by creating a special Snapshot called a consistency point every few seconds. Unlike other Snapshots, a consistency point has no name, and it is not accessible through NFS. Like all Snapshots, a consistency point is a completely self-consistent image of the entire file system. When WAFL

restarts, it simply reverts to the most recent consistency point. This allows a FAS server to reboot in about a minute even with 20 GB or more of data in its single partition. Between consistency points, WAFL writes data to disk, but it only writes data to blocks that are not in use, so the tree of blocks on behalf of the most recent consistency point remains completely unchanged. WAFL processes hundreds or thousands of NFS requests between consistency points, so the on-disk image of the file system remains the same for many seconds until WAFL writes a new consistency point, at which time the on-disk image advances atomically to a new state that reflects the changes made by the new requests. Although this technique is unusual for a UNIX file system, it is well known for databases. Even in databases it is unusual to write as many operations at one time as WAFL does in its consistency points. WAFL uses non-volatile RAM (NVRAM) to keep a log of NFS requests it has processed since the last consistency point. (NVRAM is special memory with batteries that allow it to store data even when system power is off.) After an unclean shutdown, WAFL replays any requests in the log to prevent them from being lost. When a FAServer shuts down normally, it creates one last consistency point after suspending NFS service. Thus, on a clean shutdown the NVRAM doesn't contain any unprocessed NFS requests, and it is turned off to increase its battery life. WAFL separates the NVRAM into two different logs. When one log gets filled, WAFL triggers to the other log and initiates writing a consistency point to save the changes from the initial data log safely on storage. WAFL schedules a consistency point every 10 seconds, even if the log is not full, to prevent the on-disk image of the file system from getting too far out of date. Logging NFS requests to NVRAM has several advantages over the more common technique of using NVRAM to cache writes at the disk driver layer. Processing an NFS request and caching the resulting disk writes generally takes much more NVRAM than simply logging the information required to replay the request. For instance, to move a file from one directory to

another, the file system must update the contents and inodes of both the source and target directories. In FFS, where blocks are 8 KB each, this uses 32 KB of cache space. WAFL uses about 150 bytes to log the information needed to replay a rename operation. Rename—with its factor of 200 difference in NVRAM usage—is an extreme case, but even for a simple 8 KB write, caching disk blocks will consume 8 KB for the data, 8 KB for the inode update, and— for large files—another 8 KB for the indirect block. WAFL logs just the 8 KB of data along with about 120 bytes of header information. With a typical mix of NFS operations, WAFL can store more than 1000 operations per megabyte of NVRAM.

Using NVRAM as a cache of unwritten disk blocks turns it into an integral part of the disk subsystem. An NVRAM failure can corrupt the file system in ways that fsck (file system consistency check) cannot detect or repair. If something goes wrong with WAFL's NVRAM, WAFL may lose a few NFS requests, but the on-disk image of the file system remains completely self-consistent. This is important because NVRAM is reliable, but not as reliable as a RAID disk array. A final advantage of logging NFS requests is that it improves NFS response times. To reply to an NFS request, a file system without any NVRAM must update its in-memory data structures, allocate disk space for new data, and wait for all modified data to reach disk. A file system with an NVRAM write cache does all the same steps, except that it copies modified data into NVRAM instead of waiting for the data to reach disk. WAFL can reply to an NFS request much more quickly because it need only update its in-memory data structures and log the request. It does not allocate disk space for new data or copy modified data to NVRAM.

CHAPTER 3

PROPOSED FRAMEWORK

We propose a novel Secure Data Migration framework which enables the enterprises to transfer the data from one Cloud to the other Cloud without any issues faster than the time taken to transfer from traditional Data Storage Centers to the Cloud. Also includes a Data Logging Security framework which maintains the Data Integrity throughout the migration process from Cloud to Cloud. Following are the major modules of the proposed framework:

3.1 Data Logging Framework with Enhanced Security

This framework enables the security within the cloud platform and our framework. If there is any unauthorized user accessing the data in the cloud or manipulating the data in the cloud, the framework alerts the data owner that there is some unauthorized access and it blocks the user to access the information from there on. If there is authorized user, then the framework lets them access data.

3.1.1 Major Components

Using Java programing language, major modules built in/for this work include: data owner, client (i.e., user), Cloud service provider, logger, and log harmonizer which allow users access to the log files.

Data Owner

The data owner uploads the data in the Cloud server. A new end-user can enroll with the service provider and create a new client that can securely upload the files and store it. For security purpose, the data owner encrypts and enhances the security of the data file and then the instance is saved in the Cloud. The data owner can have capabilities of manipulating the encrypted data file. And the

data owner can set the privileges to the encrypted data file. The data owner puts all the files into the Java archive file and then transfers the Java archive file to the Cloud. The data owner receives details as how to use the data record.

Client

In client module, the client registers with the data owner and thus the information is shared with the Cloud service provider by requesting for the data record. If the information provided to the Cloud service provider is correct, then the access to data or information will be provided to the client. As the client requests for the data record, the log file generated by the Cloud is sent to the data owner for the accountability of data record. The flow of a data record is illustrated in Figure 25.

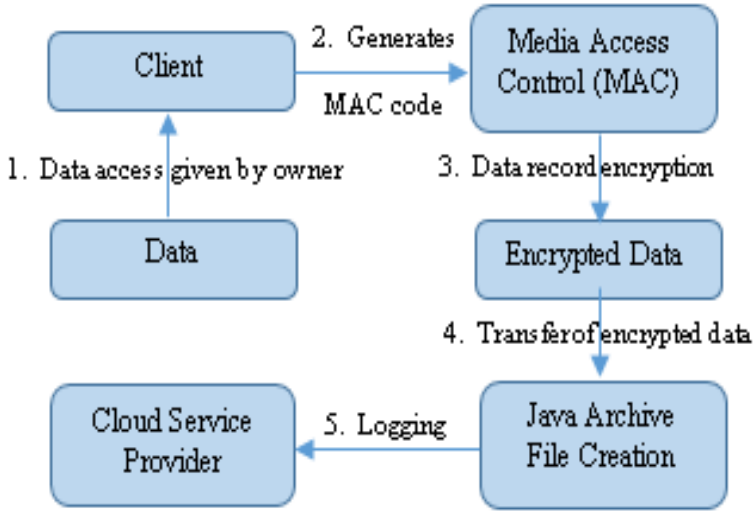


Figure 25. Data Record Flow within the framework module.

Cloud Service Provider

The Cloud service provider receives requests and provides services for the data owners and only to the registered clients. The Java archive files created by the data owner are posted on the Cloud. The Cloud data logging framework consists of two major components, the first being the logger

and the second being log harmonizer. The logger component handles instance of the user-data. The logger is also responsible for logging access to that instance of data. The log harmonizer forms the central constituent which allows the user access to the log files.

Logger and Harmonizer

The purpose of a logger and its harmonizer is to automatically log the access information of the data records by encrypting the log record using public key of the data owner. The logger periodically sends log records to the log harmonizer. In addition, the log harmonizer sends the log records to the data owner periodically.

3.1.2 Architecture and Work Flow

The data owner (see Figure 26) sends data, along with any policies such as access control policy that s/he wants to enforce, enclosed in Java archive files to Cloud service providers. Any access to data starts an automated and authenticated logging mechanism centralized to the Java archives.

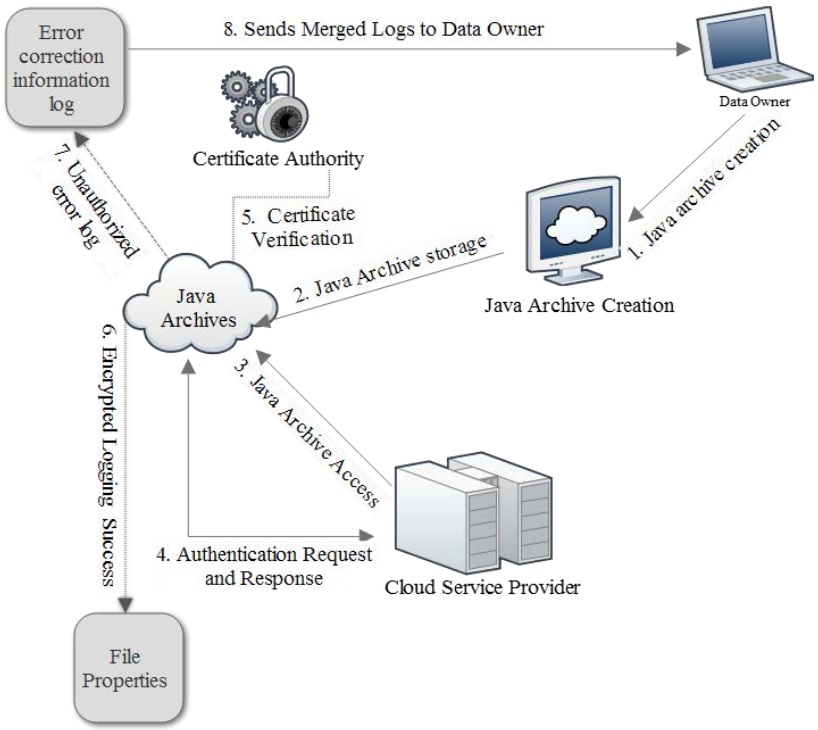


Figure 26. A Highly Decentralized data logging framework.

The logging data framework uses the identity based encryption for generating the private key and public key generator for generating the private key which can be compromised. To overcome this problem, RSA and MD5 algorithms, based on random primary numbers, are used in this work. The framework also uses hierarchical encryption and decryption of both data record and log record with different approaches.

The data owner registers with the Cloud service provider and receives the owner unique ID and the keys. A sample data owner registration is illustrated in Figure 27.

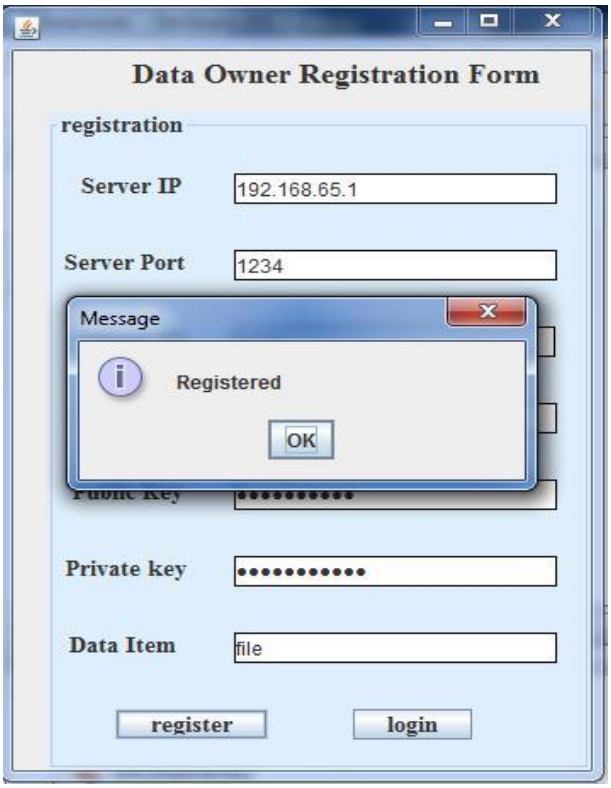


Figure 27. A Sample Registration of Data Owner.

The original data owner logins by providing the owner ID and server IP address. Once the owner logins, it provides the access privileges for the registered client which gets stored in a file (say, “access.txt”). The media access control code for the data record for a client is generated and

stored. The data record is encrypted using the shared key. That shared key is stored in a file (say, "password.txt") and the same is used for decryption. Once the data record is encrypted, the Java archive file is created which comprises of the encrypted file, password file, and the access file. The Java Archive (JAR) file is saved as compressed ZIP files. Then the Java archive file is transferred to the client service provider as the outer Java archive. The control flow is represented in Figure 28.

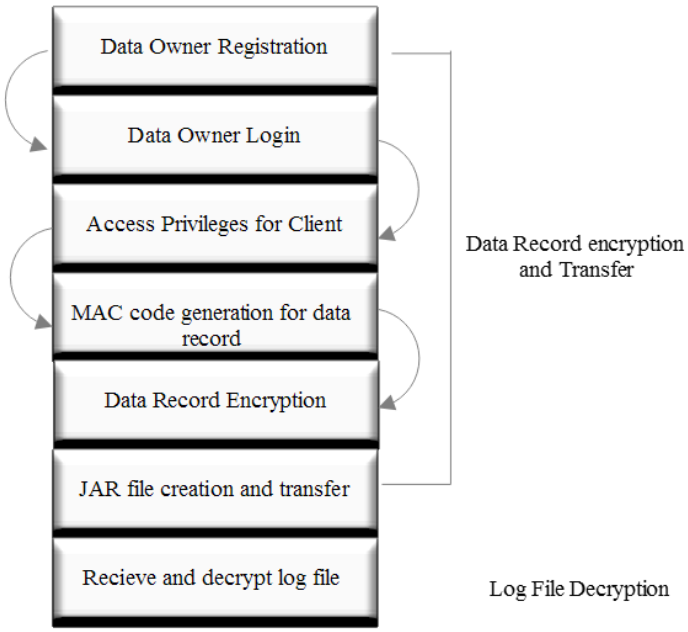


Figure 28. Control Flow of Data Owner Module.

The Cloud service provider starts providing the service and responds to the request of a data owner. The data owner registers with the Cloud service provider. Once the registration is completed, the data owner logins and transfers the Java archive files which contains the encrypted data record and "password.txt" shared key. Once the Java archive outer JAR receives the service provider structure, the inner JAR files (where it extracts the files from the archive file) are stored in the database for further use during verification of client. Flow diagram is represented in Figure 29.

If the client is verified as a privileged user, then the Cloud service provider automatically logs the access to an encrypted file (say, “retrieval.txt”) thus transfers to the data owner by using owner ID and public key. The Cloud service provider decrypts the Accessed/downloaded file using the shared key (presented in “password.txt”) and transfers the data record to client.

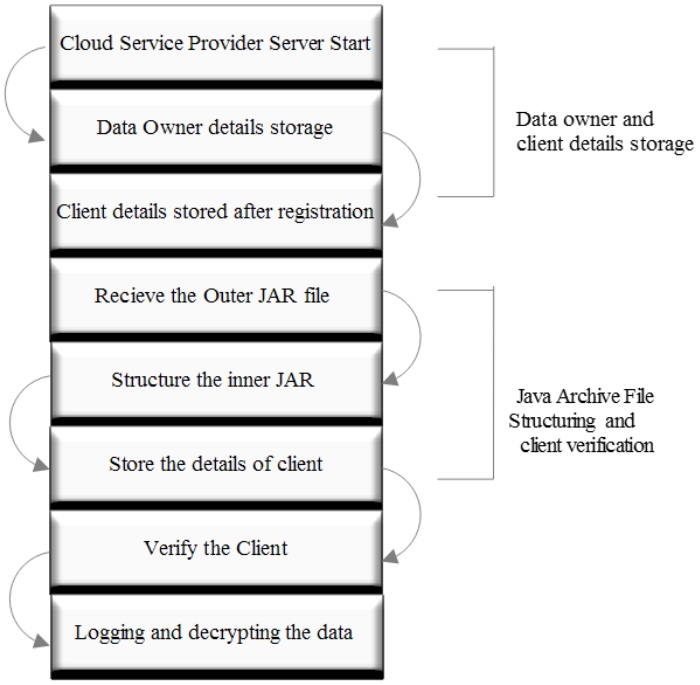


Figure 29. Cloud Service Provider Module work flow.

The client registers with the data owner and gets the client ID and a private key. The client logins to the Cloud service provider. Login is successful only if the input provided by the client and the details stored in the database are matching. Once the client logins, the client is verified by the Cloud service provider as to whether the client is a privileged user or not. Once the client is verified the client requests for the data record and the request is automatically logged by the service provider. Then the client receives the decrypted data record from Cloud service supplier and downloads the data record to “mydata.txt” at the client side. Figure 30 represents the flow diagram of client module.

For authenticating the users and the Cloud service provider, we generate keys. The public and private keys are generated using RSA algorithm, the prime numbers selected randomly using the "random()" function where the limits are specified and the prime number is selected within the range.

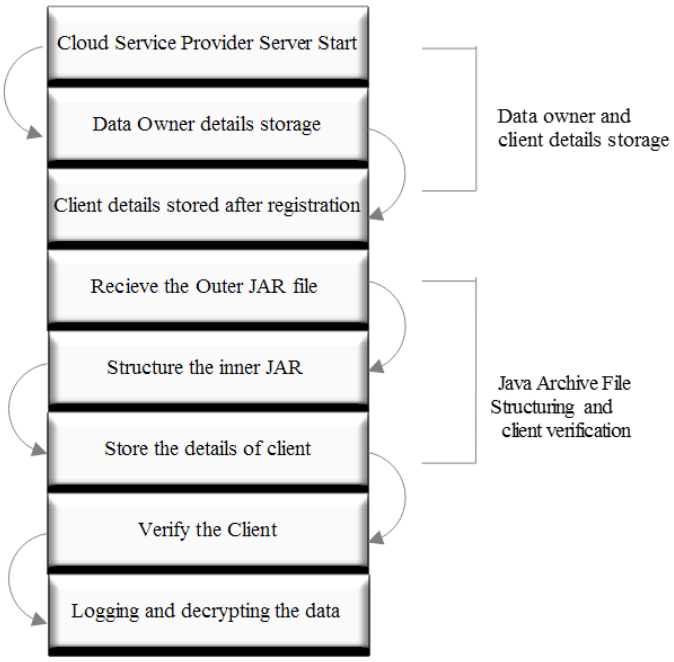


Figure 30. Work flow of Client Module

The MD5 algorithm is a widely used function that produces a 128-bit hash value, usually indicated in text format as a 32-digit hexadecimal number. MD5 has been deployed in a wide variety of cryptographic applications and is also used to verify data integrity.

The encryption and decryption of the data record and the log record are done using the Advanced Encryption Standard (AES) algorithm. AES is a symmetric encryption algorithm, designed to be efficient in hardware as well as software. AES algorithm supports a block length of 12 bits and key lengths of 128, 192, and 256 bits. In this work, the AES algorithm generates 128-bit long key which is used to generate the cipher file from a plain file. The results of the encryption will appear in a base-64 encoded value to prevent character encoding problems. If one wants to decrypt a text, s/he

needs to be sure that it is encoded in base-64 and encrypted with AES algorithm. The decryption of the encrypted text is possible only if one knows the right shared key. The password is stored in "password.txt" and shared between the data owner and Cloud service provider only.

A line-by-line security of file authentication (through the RSA and MD5 algorithms) is used to create a dynamic and secure Cloud environment. According to the experimental results, the data logging framework has potential to decrease unauthorized access. Experimental results also suggest that the data logging framework may help decrease data theft and data loss.

To achieve the best solution, we are considering the following scenario of hybrid clouds:

When the enterprise using Cloud 'A' is not satisfied with the performance of 'A' they would need to migrate to Cloud 'B'. Initially they undergo all the steps such as breaking up the contract and finish all the formalities. Problem arises when the secured data with Cloud 'A' is transferred to Cloud 'B' whether they got the complete data or not. So, to make sure that the data transferred is successfully with enough security in cloud computing it might be a huge task. To make this complex task into a simple task our solution is as follows.

Let 'A' be the source cloud, 'B' be the destination cloud 'X' be the backup cloud. Here we assume 'X' to be some number of other brokers present in the back up cloud; where we have the option to opt the best backup cloud based on our convenience.

- First the enterprise contacts 'A' support team stating that he is not satisfied with the service and he wants to move to his desired cloud provider say 'B'.
- Now the technical team of cloud 'A' will check the amount of data present for ex: 1.1 TB in cloud S. Their duty is to make sure that the data transferred from cloud 'A' must be successfully transmitted to Cloud 'B'.

- We assume in this step that support team gives the option to the enterprise, to choose their own back up cloud they desire.
- In this case, we assume cloud ‘M’ to be migration cloud, where M is selected from the set of backup clouds ‘X’.
- Once the enterprise selects its back up cloud ‘M’ from ‘T’ and the support team of ‘A’ will inform the ‘M’. Where cloud ‘M’ will take care of all the data security.
- Later, cloud ‘M’ will migrate all the information to cloud ‘B’.
- Thus, all the data is successfully transmitted from cloud ‘A’ to cloud ‘B’ with ease.

3.2 Cloud Migration Framework Architecture

The following are the main components of the proposed API which is used to migrate the cloud from one cloud service to the other service provider:

3.2.1 Adornment Graph Algorithm

We solve the problem of transferring all the data with the help of Adornment Graph (AG) algorithm. Graph AG (M, X) = (N, L), where N is a set of nodes, ‘M’ be a mediator and ‘L’ be set of labels. There is one node for each source that pertains to a small target ‘X’. Consider a source S1 with various problems. Consider the below example

of Source ‘S’ with 5 relations S(a,b,c,d,e). Here a, b, c, d, e denotes various issues faced by the cloud in Cloud computing as shown in the Figure 31. Each source is known with its template; the source is denoted with its superscript; for example, source is known with template nfnff is denoted by Sfnfff.

$$S= S^{fnfff}(a,b,c,d,e)$$

We observe that source has various problems as shown in Fig 32, where Mediator should take the initiative to fix the issues which source is facing. Consider a Source ‘S’ with three relations

S(a,b,c,d,e) and M(a',b,c',d',e') where b is the type of issue and a',c', d'and e' are considered to be that there are no issues .

$$S = S_{fnf}(a,b,c)$$

$$M = M_{fffff}(a', b, c', d', e')$$

Where 'a' - Unknown Physical Location

'b'- Security

'c' - Blind Trust

'd' - Shared Resources

'e' - Legal Issues

F	N	F	F	F
a	b	C	d	e

Where, N - Not Fixed Issue | F- Fixed Issue

Figure 31. Template of Source Cloud (S1).

From Figure 32 we observe that source 'S' has a security issue. Immediately source will notify its security problem with 'b' state. Here the mediator takes the initiative to fix the issue. Mediator takes the help of IaaS, SaaS and PaaS in order to fix the issue. The fact is that in real time no one uses all the three platforms effectively; they might use one among the three platforms due to the above fact, it is very complicated to resolve the issue or migrate the data.

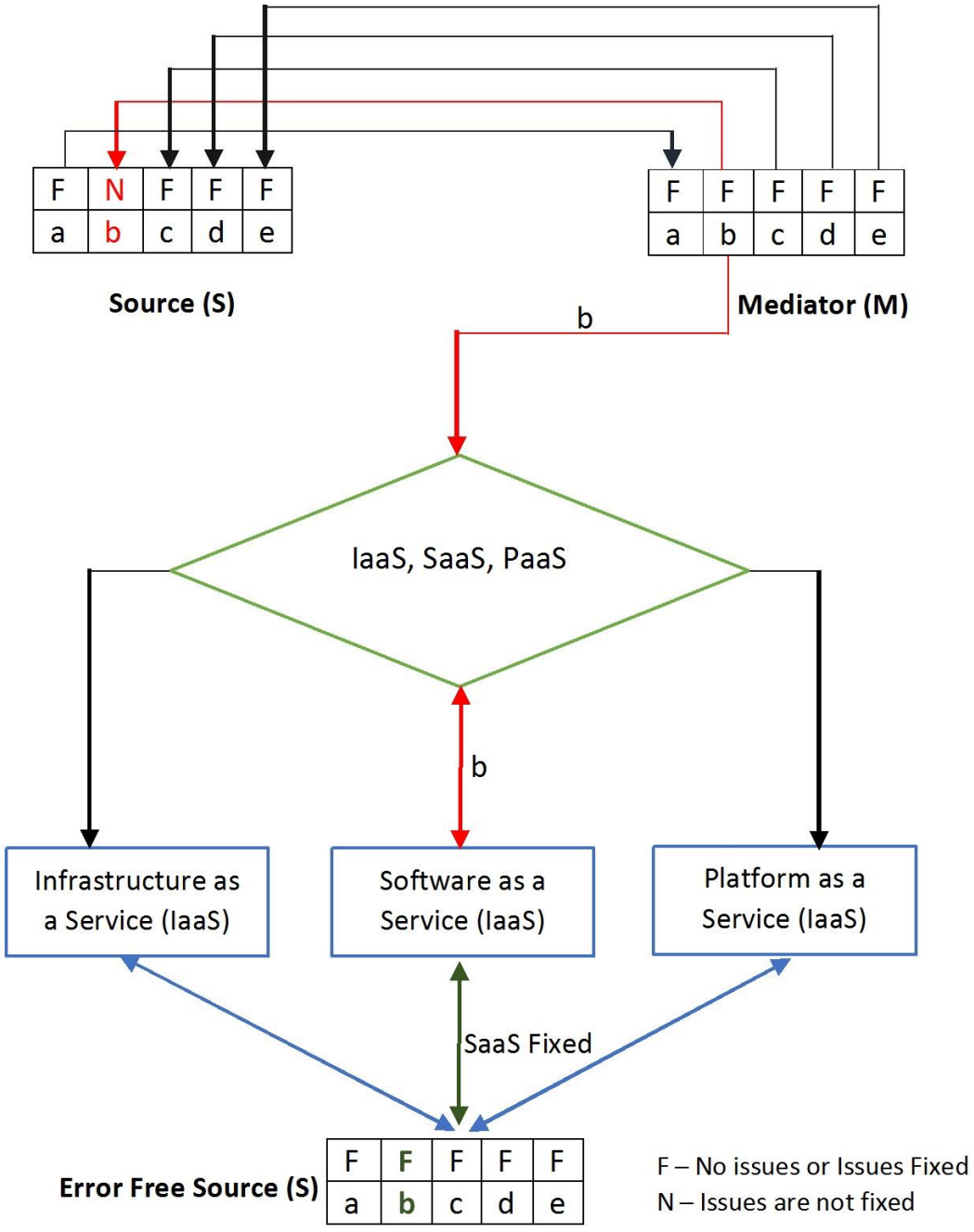


Figure 32. Adornment Graph for Security Issues in Source Cloud being solved.

We tend to use all the three platforms effectively with the base of AWS cloud migration technique. The relation between the source, mediator and destination is as M (a,b,c,d,e) which has the capability to fix any problem, S(b) source which has security issues which has to be fixed by the mediator (M). Unless the problem is fixed, cloud cannot migrate the data.

Let R=(S) U (M)

Where, U - Union R – Relation

S= Sfnf (a,b,c)

R= S*fnf* (b) U M*fffff*

The above steps are repeated for destination (D). Thus, issues are solved with the help of union views.

3.2.2 Migration API

The Migration API (as shown in Fig 33) provides a unified programming platform to abstract from the differences among provider API implementations. For enterprises, using this API prevents their application from being hard-wired to a specific cloud service provider. The API can build on available cloud provider abstraction APIs. Although these deals mostly with key value stores and computing services, in concept, all services can be covered that are abstract enough for more than one provider to provide and whose specific APIs don’t change too much, conceptually.

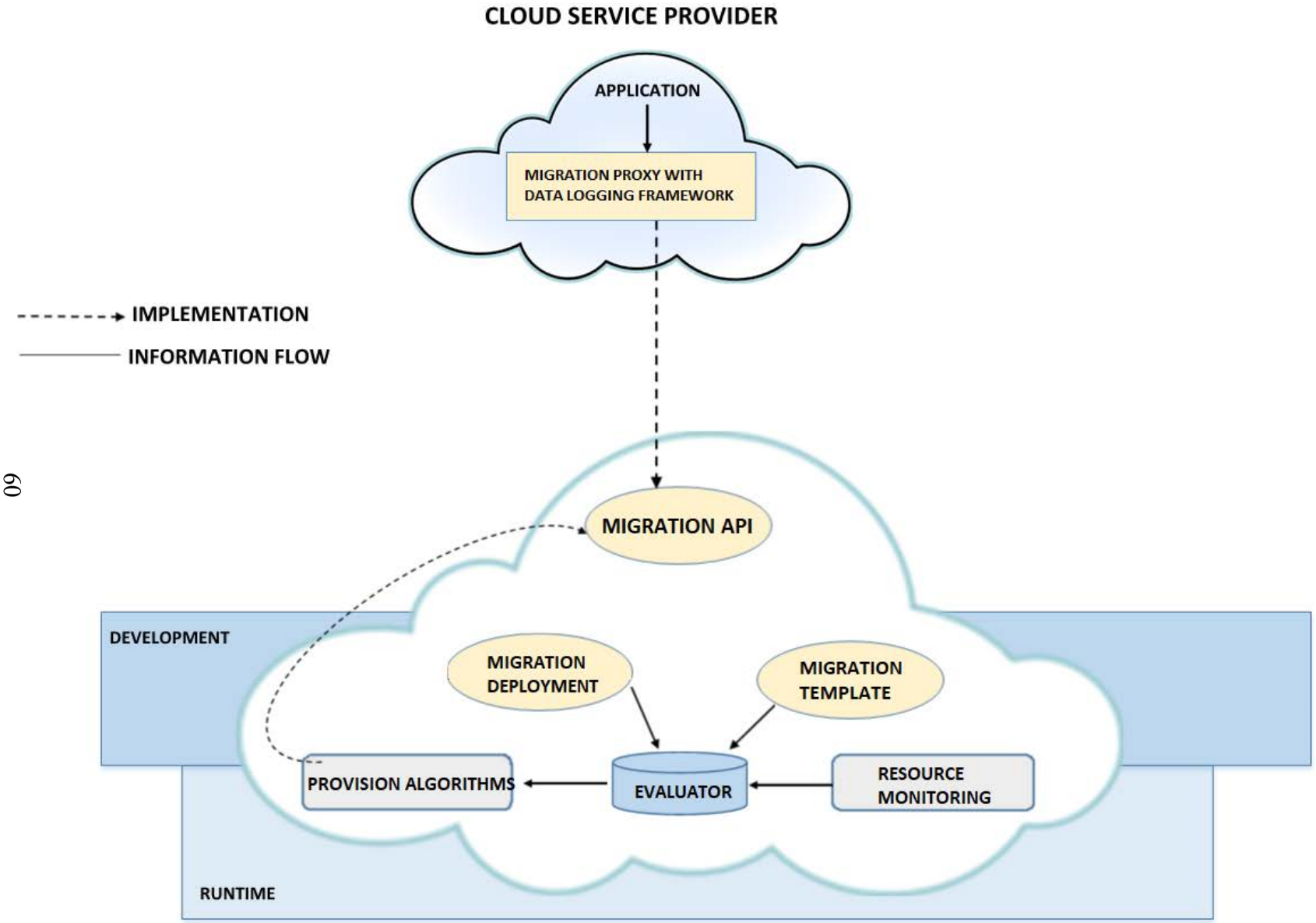


Figure 33. Cloud Migration Framework Architecture with NetApp's NVRAM / WAFL.

3.2.3 Migration Template

We describe the cloud services necessary to run an application using migration templates (as shown in Fig 33). We can specify service types with additional features, and a graph method illustrates the correlation and functional dependencies between services. We create the templates using a simple domain-specific language (DSL), letting other developers concisely specify required resources. Migration Resource definitions are based on a hierarchical composition model; thus, developers can develop configurable and renewable template components, which enable them and their teams to share and reuse common migration templates in different projects.

Using the DSL, we model enterprises' application components and their basic run time requirements, like Processor Unit, memory, and Input Output capacities, as well as dependencies. The provisioning algorithms uses the filled element connections to determine the application's best deployment configuration. Moreover, migration resource templates allow developers to determine factors based on costs, component proximity, and geographical distribution.

3.2.4 Migration and Deployment Methods

Deployment methods (as shown in Figure 33) are an important part for automation in the migration infrastructure. Such methods allow for configurable deployment of the application, including installing packages, starting required services, supervising packages, application criteria, and creating links between inter related components. Automation tools give an extensive set of objectives that are directly integrated into the meta cloud environment. Migration recipes go one step ahead and define how to migrate an enterprise application during run time migration recipes only define initial deployment and transferring; the provisioning algorithms and the migration proxy executes the actual process using the automation tools.

3.2.5 Migration Proxy

The migration API (as shown in Figure 33) provides proxy objects, which are setup with the application and execute on the provided cloud resources. They serve as negotiators between the application and the cloud service provider. These proxies expose the migration API to the application, convert application requests into cloud provider specific requests, and sends them to the specific cloud services. Proxies provide a way to run deployment and migration methods triggered by the migration framework's strategy. Proxy objects sends Quality of Service statistics to the service monitoring component running within the framework.

3.2.6 Resource Monitoring

On an application's demand, the resource monitoring element (as shown in Figure 33) receives data collected by migration proxies about the resources they're utilizing. The component filters and executes the data and then captures them on the knowledge base for further querying. This helps developing comprehensive Quality of Service report about cloud service providers and the services they provide, including quick response time, resources availability, and more service-specific requirements.

3.2.7 Provisioning Algorithms

The provision algorithms module (as shown in Figure 33) primarily matches an application's cloud service elements to actual cloud service providers. It checks and ranks cloud services based on data present in the evaluator. The initial deployment decision is based on the migration templates, pointing the requirement of resources of an application, together with Quality of Service and pricing policy about service providers. The final yield is a list of possible cloud provider's list ranked according to the expected QoS and costs.

3.2.8 Evaluator

The evaluator (as shown in Figure 33) stores data about cloud provider services, their costs and QoS, and information necessary to estimate migration costs. It also stores enterprise provided migration resource templates and migration or deployment methods. The evaluator indicates which cloud providers are eligible for a certain enterprise. These usually comprise all providers the enterprise has an account with and service providers that provides possibilities for creating child accounts on the fly. Several information sources contribute to the evaluator: migration proxies regularly send data about application behavior and cloud service rank. Individuals can add cloud service providers' costing and features manually or use crawling techniques that can get this information automatically.

3.2.9 Optimized Tsunami Protocol

Tsunami is one of the User Datagram Protocol -based transfer protocols that is used for high speed transfer over network paths that have a high bandwidth-delay product. Tsunami performs a file transfer by dividing the file into multiple numbered blocks of usually 32kB size. Communication between the client and server applications flows over a low bandwidth TCP connection. The bulk data is transferred over UDP. Most of the protocol background is based on the client code - the server just sends out all blocks, and re-sends blocks that the client requests. The client specifies almost all parameters of the transfer, such as the requested file name, target data rate, block size, target port, congestion behavior, etc, and controls which blocks are requested from the server and when these requests are sent [90]. We modify Tsunami protocol to obtain high speeds of at least 649Mbps which is higher than the default Tsunami protocol.

```
00:07:37.007 29200    0.09M   651.0Mbps    0.1% 37967250    36.2G   649.0Mbps    0.0%
   19      0 488668392         19      6273 --
00:07:37.358 29200    0.42M   651.3Mbps    0.0% 37996450    36.2G   649.0Mbps    0.0%
    2      0 488639192          2      6275 --
00:07:37.708 29200    0.04M   651.0Mbps    0.0% 38025650    36.3G   649.0Mbps    0.0%
    8      0 488609992          8      6283 --
00:07:38.059 29200    0.18M   651.1Mbps    0.0% 38054850    36.3G   649.1Mbps    0.0%
    9      0 488580792          9      6292 --
00:07:38.409 29200    0.20M   651.4Mbps    0.0% 38084050    36.3G   649.1Mbps    0.0%
    2      0 488551592          2      6294 --
00:07:38.760 29200    0.04M   651.2Mbps    0.0% 38113250    36.3G   649.1Mbps    0.0%
    2      0 488522392          2      6296 --
00:07:39.110 29200    0.04M   651.3Mbps    0.0% 38142450    36.4G   649.1Mbps    0.0%
    0      0 488493192          0      6296 --
00:07:39.461 29200    0.00M   651.1Mbps    0.0% 38171650    36.4G   649.1Mbps    0.0%
```

Figure 34. Maximum Speed Achieved using Tsunami Protocol 649.1Mbps

Setup

An EC2 instance with at least 10Gbit Ethernet network would be better requirement to achieve higher transfer speed. TCP 22 and TCP/ UDP 46224 needs to be opened between server and client for communication and data transfer.

- *sudo apt-get install git gcc*
- *sudo apt-get install automake autoconf*
- *cd tsunami-udp*
- *. / recompile.sh*
- *sudo make install*

Old Cloud acting as Server Terminal: Start the process as follows

tsunamid --port 46224 * # (*Serves all files from current directory for copy*)

New Cloud Terminal acting as Client: Start the Transfer as follows

tsunami connect [server] get * # (*copies all files served to current directory*)

CHAPTER 4

EXPERIMENTAL SETUP

In this chapter, we simulate the entire cloud environment and try to transfer data from one system to another system.

Assumptions

Assign the port number for the tomcat server to be 8888 with “admin” as the username and the password, and for MySQL we use “root” as username and password. Now, connect two systems using Logical Area Network(LAN) and set their system IP addresses as 10.0.0.100 and 10.0.0.110 respectively. We have set these IP addresses so that we don’t have to change the IP addresses in the developed application (code). Later, once the system is configured we start simulating the data transfer. The request flow is shown in Figure 35.

4.1 Migration Modules

In the proposed application framework, we have three application modules as follows:

- Receive module
- Cloud Application (Proposed solution)
- Data Transfer module

4.1.1 Receive Module

The main purpose of the receive module is check if the connection between previous cloud service provider and the new cloud service provider is successful. And it also requests the previous cloud provider to send the data transfer application from its server to new cloud service provider. When we run the receive module, it asks the server to start sending the data transfer application to the new cloud so that the new cloud user can start receiving their old data from their previous

cloud. Here, we consider the server to be the previous cloud service provider. The receive module makes a request to the cloud application.

4.1.2 Cloud Application

The administrator of the previous cloud service provider starts the Cloud application module securely with their login credentials. If there is any unauthorized access to the cloud, then the system triggers an error message and exits. Once the login is successful, we click on the migration templates and configure them according to the new cloud service provider's requirement. After creating all the migration templates, we can add new providers who provide the same services for lesser price. And the users get the authority to choose the best service provider needed per their requirements. Once, the user selects the new service provider, the data transfer module is called and the data transfer takes place.

4.1.3 Data Transfer Module

The data transfer application requires three inputs from the admin of the previous cloud: IP address of the source (previous cloud) and destination cloud (new cloud service provider), and the folder name from the old cloud. Once the system gives a log that the folder was successfully sent, the receive application in the new cloud can check the data or folder received from the old cloud service provider. In the data transfer module, we use the NetApp NVRAM and NetApp WAFL hardware methodology as shown in Figure 35.

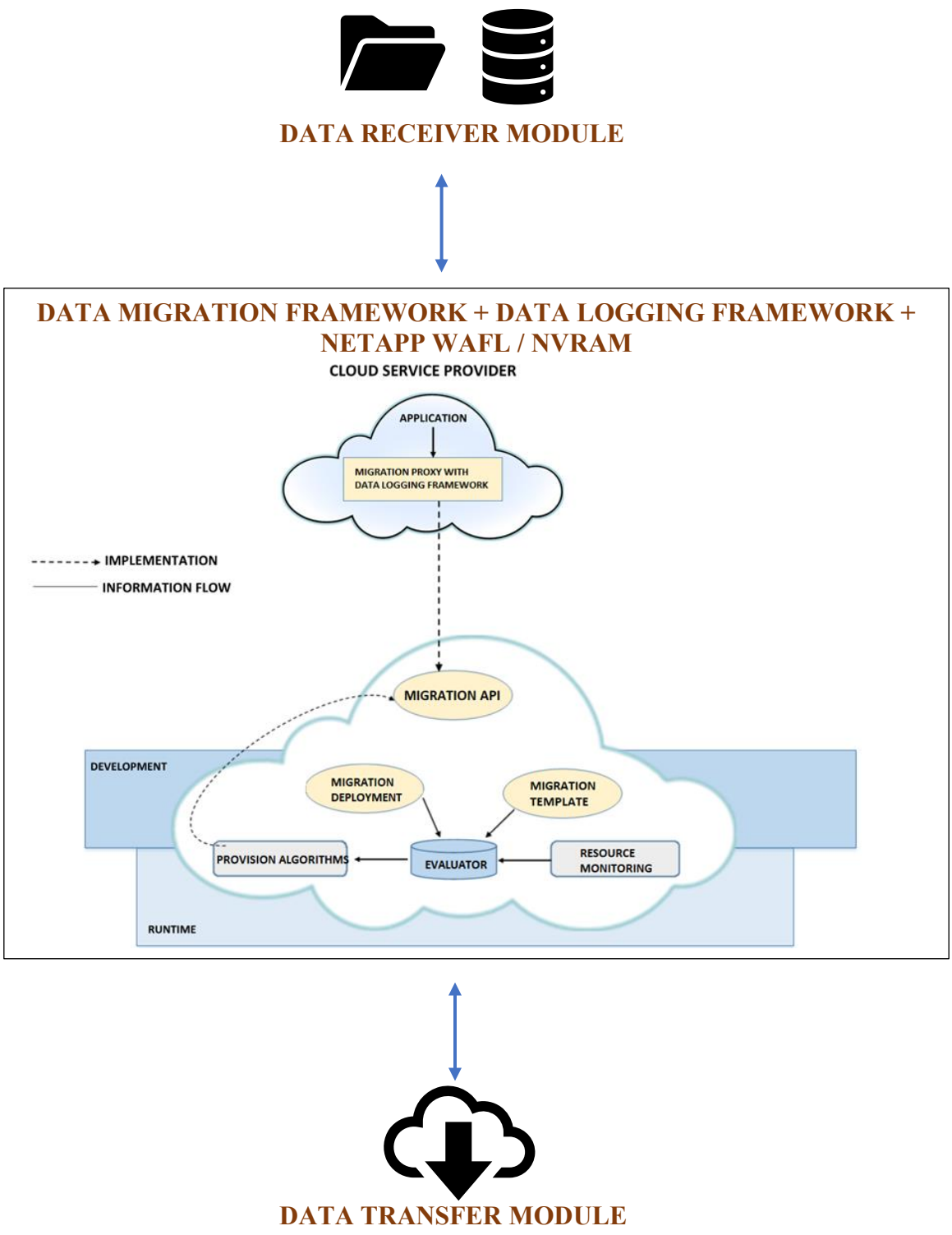


Figure 35. Skeleton of Proposed Framework and brief work flow

4.2 Work Flow

When we start the cloud migration framework, firstly we make sure that the Source Cloud and Destination clouds are compatible to our framework requirements. Secondly, In the source cloud we start the Receiver module. In receiver module, we have our cloud migration framework which determines the issues which would be occurring while data transfer. And if any issues are found, the cloud migration framework with help of NVRAM solves by IaaS, SaaS and PaaS cloud application as shown in Fig 36.

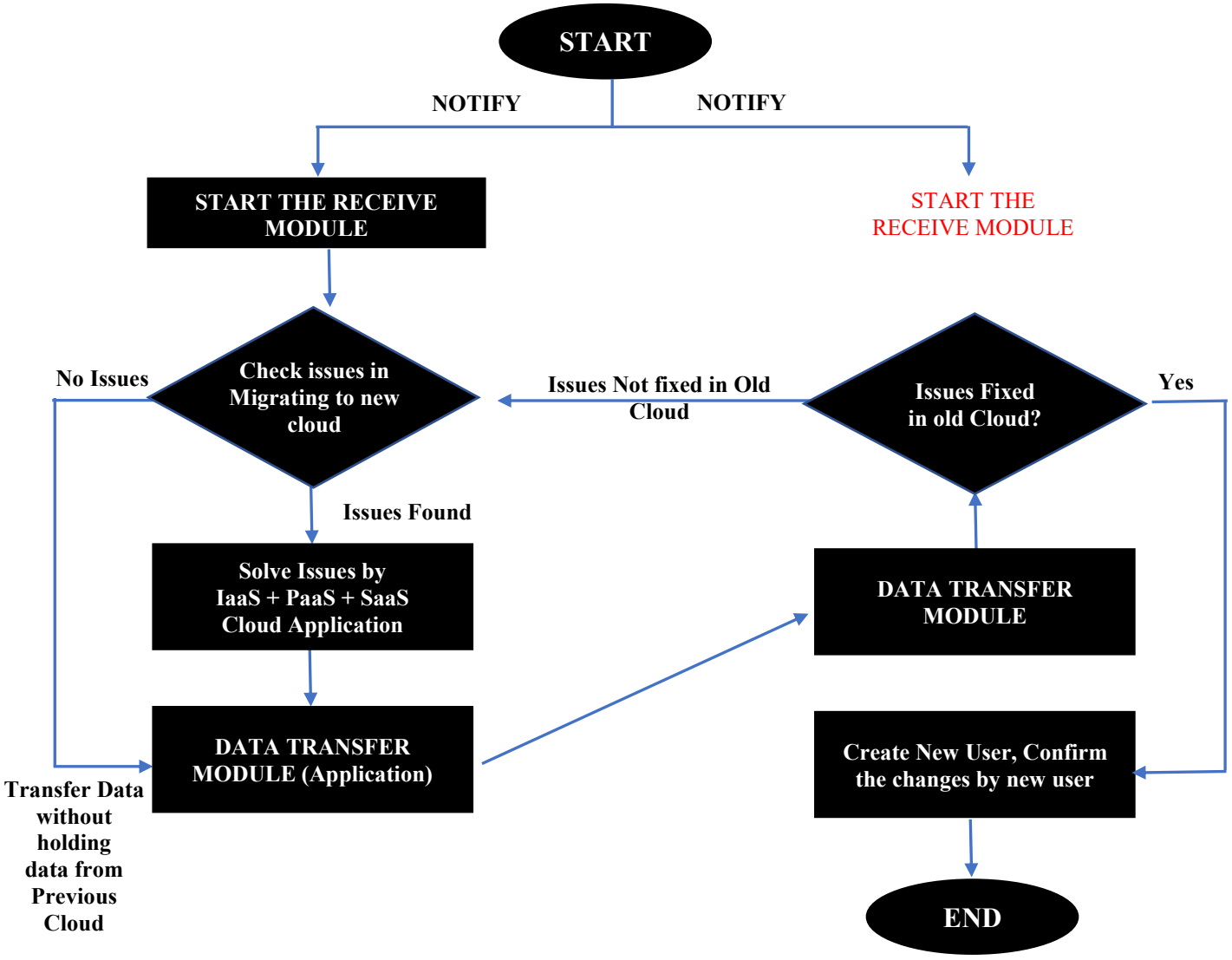


Figure 36. Work Flow in Cloud Migration Framework.

Then after fixing the issues the module initiates the Data Transfer process using the Data Transfer Module which has WAFL and NVRAM to make sure that the data integrity is maintained, and the data is not lost. And the data is ready to be transmitted to the destination cloud. Now, if there is no issue then the data is directly transmitted to destination. Once the data is ready to be transmitted to the Destination cloud, the Receiver module in Destination is activated and checks for issues in receiving the data from Source cloud. If there is any issue that is not fixed in Source cloud the control is transferred back to Source cloud to rectify the issues. And if all the issues are fixed, we create a new user and confirm the changes by the user.

Formula for calculating Transfer time theoretically

As part of the experiment, data sizes from 1 MB, 10MB, 100MB, 1000MB, 10000MB, 100000MB and 1000000MB were used as use cases. The transfer rate slightly increases as the size of the application increases and the amount of data increases. But, the time taken for transfer is usually less than the time taken for a traditional transfer. Once the migration is successful we calculate the time taken for transfer. The time taken for transfer of data from storage device to cloud is: $D = (n)/(Mbps * 125 * 1000 * U * 60sec * 60min * 24hrs)$

This formula tells the time taken to migrate from a traditional system to cloud using AWS and proposed framework. Where ‘D’ is the total number of days, ‘n’ is the number of bytes, ‘U’ is network utilization. For example, if you have a connection (1.8Mbps) and 1TB (1024 * 1024 * 1024 * 1024 bytes) to migrate to cloud the theoretical minimum time it would take to load over your network connection at 85% network utilization is 79 days. This is what a traditional technique takes to migrate from physical storage to cloud of enterprise (making sure the platform dependencies and all other factors) theoretically, and is secure enough, and save costs for an enterprise practically on real time.

CHAPTER 5

RESULTS

In this Chapter, we simulate the proposed cloud migration framework integrated with the Data logging framework for enhanced security and NetApp WAFL/NVRAM. With different amounts of data and at different bandwidths we tabulate the findings below.

5.1 Data Logging Framework with Enhanced Security

In this section, we summarize some test cases that are used to validate the proposed data logging framework. As shown in Table 3, ten different test cases are considered to test important modules such as the data owner and client/user. Each case was tested at least ten times.

- For Test Case 1 (login for data owner), ten tests are performed; five tests with valid Server IP addresses and valid Owner IDs and five tests with invalid Server IP addresses and/or invalid Owner IDs. As shown in Table 3, data owners successfully logged in five times (with valid Server IP and valid Owner ID) and failed five times.
- Test Case 2 (login for client) is observed by giving server IP address and client ID as inputs. Client login is successful six times with valid credentials and unsuccessful six times with invalid credentials (as shown in the Table 3).
- For Test Case 3 (key generation), random variables are generated by RSA algorithm and Private and Public keys are obtained as expected.
- Test Case 4 (access privilege to storage) is to test the clients' privileges to the stored data. A client, who may login successfully, can either Read, Write, or both. The information about privileges is stored in JAR files. Test Case 4 produces JAR files every time.
- Test Case 5 (encryption of data record) takes a file, a shared key, and some cipher texts as inputs. These inputs are used to test encryption. If there is any invalid input, the encryption

should fail. As shown in Table 3, Test Case 5 passed six times and failed six times as expected.

- For Test Case 6 (JAR files transfer and automatic logging), server IP address, JAR file names, data file name, client ID, client name, owner ID, and access privileges are considered as inputs. The proposed framework stores the information in "access.txt" and "retrieval.txt". If the information is stored successfully then a test passes, or it fails. As expected, tests pass five times and fails five times.
- For Test Case 7 (log file transfer), inputs are the owner ID and public key (generated by RSA algorithm). If the log file transfers successfully a test passes, otherwise it fails. These tests pass five times and fails five times as supposed.
- Inputs for Test Case 8 (decryption of data record) are data file name, shared key, and cipher label. For valid inputs, the data file should be decrypted. If there is any unusual input the decryption should fail. Test outcomes are as anticipated.
- Test Cases 9 and 10 (data record integrity check) are to check if there is any unauthorized access to the data file. The data file name, owner IDs, client IDs, and access privileges are given as inputs. The input data file is analyzed using other input parameters. If there is no unauthorized access, a data record integrity test passes. Due to any unauthorized access to the data file and/or its contents, a test fails and the log record about the access is sent to the data owners.

TABLE. 3

VARIOUS TEST CASES TO VALIDATE THE SECURITY FRAMEWORK

Test Case	**Description**	**Input(s)**	**Output(s)**	**Remarks**
1	Login for data owner	Server IP, Owner ID	Data owner login: Pass or Fail	Five Passes, five Fails (as expected)
2	Login for client	Server IP, Client ID	Client login: Pass or Fail	Six Passes, six Fails (as expected)
3	Key Generation	Random variable RSA	Private key, public key	Keys are generated every time (as expected)
4	Access privilege to storage	Client ID, Read/Write access	JAR files	JAR files are created every time (as expected)
5	Encryption of data record	File, shared key, cipher label	Data encryption: Pass or Fail	Six Passes, six Fails (as expected)
6	JAR files transfer and automatic logging	Server IP, data file name, JAR file names, client ID, client name, owner ID, access privileges	Stored in "access.txt" and "retrieval.txt" files: Pass or Fail	Five Passes, five Fails (as expected)
7	Log file transfer	Owner ID, public key	Log file transfer: Pass or Fail	Five Passes, five Fails (as expected)
8	Decryption of data record	Data file name, shared key, cipher label	Data file decryption: Pass or Fail	Five Passes, five Fails (as expected)
9	Data record integrity – pass	Data file name, owner IDs, client IDs, access privileges	No unauthorized access	None out of ten tests (as expected)
10	Data record integrity – failure	Data file name, owner IDs, client IDs, access privileges	Unauthorized access	All of ten tests (as expected); log records were sent to data owners

5.2 Successful Data Migration from one cloud to the another

When we simulated the traditional uploads and downloads time with 1.024Mbps bandwidth, the time taken to transfer increased as the size of the data increased. As the bandwidth increases the transfer time decreases when we compare the results in the Table 4. Now, when we simulate our proposed framework which is useful in transferring data from one cloud to another cloud, we find that the time taken to transfer from one cloud to another cloud is lesser than the time taken in traditional method of transferring data. The results shown in Table. 4 are with 10% overhead.

TABLE. 4

TRADITIONAL TRANSFER TIME VS PROPOSED FRAMEWORK TIME (1MBPS BANDWIDTH)

File Size (in Megabytes)	Transfer Time (in Seconds) EXISTING	Transfer Time (in Seconds) PROPOSED
1	8	6
10	75	70
100	851.4	821
1000	8046	7506
10000	84708	80708
100000	858348	834232

When we simulated the traditional uploads and downloads time with 500Mbps bandwidth, the time taken to transfer increased as the size of the data increased. As the bandwidth increases the transfer time decreases when we compare the results in the Table 5. Now, when we simulate our proposed framework which is useful in transferring data from one cloud to another cloud, we find that the time taken to transfer from one cloud to another cloud is lesser than the time taken in traditional method of transferring data. The results shown in Table. 5 are with 10% overhead.

TABLE. 5

TRADITIONAL TRANSFER TIME VS PROPOSED FRAMEWORK TIME (500MBPS BANDWIDTH)

File Size (in Megabytes)	Transfer Time (in Seconds) EXISTING	Transfer Time (in Seconds) PROPOSED
1	0.0125	0.0095
10	0.1525	0.0953
100	1.525	0.9536
1000	15.25	9.536
10000	152.588	95.367
100000	1525.88	953.674

When we simulated the traditional uploads and downloads time with 1Gbps bandwidth, the time taken to transfer increased as the size of the data increased. As the bandwidth increases the transfer time decreases when we compare the results in the Table 6. Now, when we simulate our proposed framework which is useful in transferring data from one cloud to another cloud, we find that the time taken to transfer from one cloud to another cloud is lesser than the time taken in traditional method of transferring data. The results shown in Table. 6 are with 10% overhead.

TABLE. 6

TRADITIONAL TRANSFER TIME VS PROPOSED FRAMEWORK TIME (1GBPS BANDWIDTH)

File Size (in Megabytes)	Transfer Time (in Seconds) EXISTING	Transfer Time (in Seconds) PROPOSED
1	0	0
10	0	0
100	0	0
1000	8	4
10000	76.4	72.4
100000	864	712.3

Using iperf in Linux we calculated the speed of upload and download with a python script (speedtest-CLI). When we compare the traditional (present technique) and the proposed framework,

the time taken by the proposed framework is relatively less when compared to the traditional way of transferring the from one source to destination (it might me web downloads too).

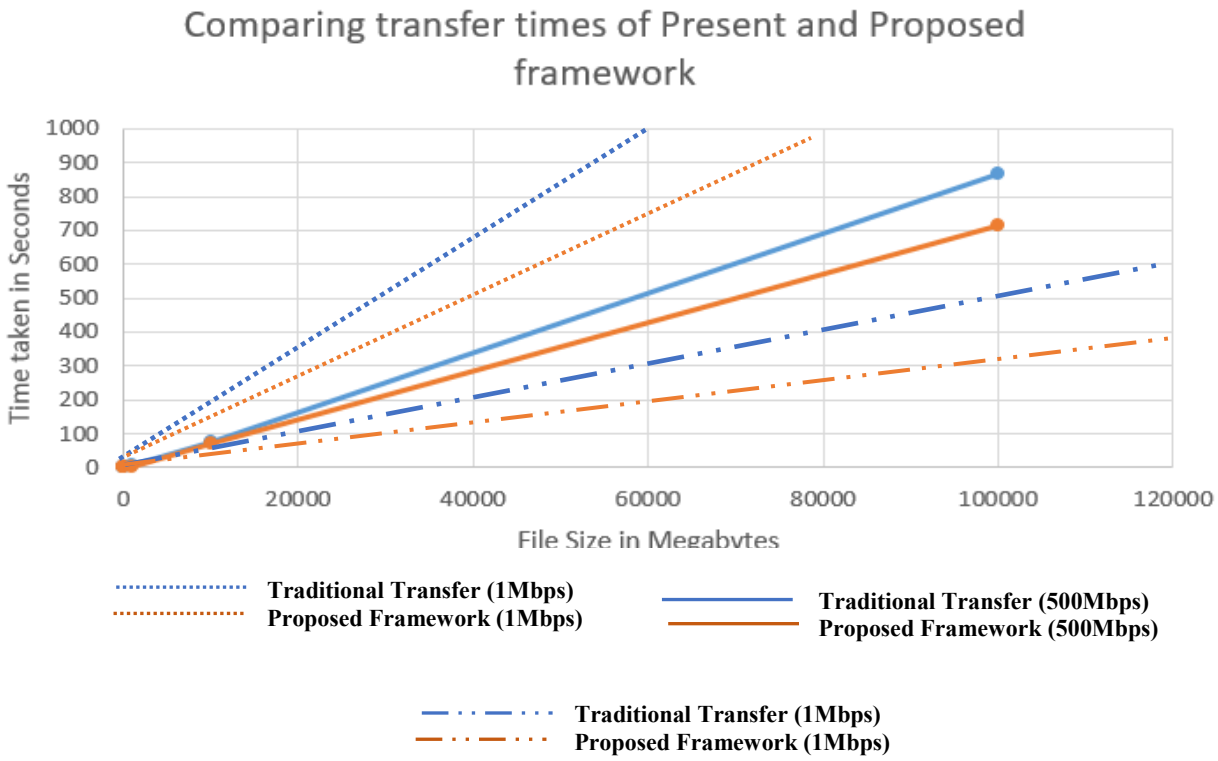


Figure 37. Comparison of Existing Vs Proposed framework for data transfer in Seconds.

5.3 Fail Cases in Data Migration from one cloud to the another

While simulating this experimental setup, we also experienced and tried to make sure that there is some disruption in network. Because, internet is the main source for using a cloud application. And when we simulated the network issue on the cloud migration framework, we observed that the data migration or the data transfer module stops sending data packets from the old cloud provider. And when we make sure that there is no network issue, the WAFL and NVRAM enables the migration framework to send the packet at which the data transfer stopped or had issue. So, we also prove to solve the data continuity problem if there is any network error occurring while the data is being transferred. But, it would take some extra time to restart the module and check for

packet count and integrity. Table 8 shows the time taken to transfer data if there is any network issue while transferring the data from old cloud service to new cloud service provider.

TABLE. 7

PROPOSED FRAMEWORK TRANSFER TIME (1GBPS BANDWIDTH) IF ANY NETWORK ISSUE PERSISTS

File Size (in Megabytes)	Transfer Time (in Seconds)	Transfer time (if any network issue occurs) in seconds
1	6	9
10	70	76
100	821	830
1000	7506	7516
10000	80708	80750
100000	834232	834310

There are other fail cases which are considered such as, if there exists a failure in data integrity and data continuity the framework takes more time to transmit the data as, it has to restart the whole receive module, check for issues and then make sure that the time slot at which the transfer failed is continued from that point to ensure there is no duplication of data packets using the Message Digest 5 algorithm and NVRAM WAFL methodology. Later we also ensured that the whole data is transferred from old cloud to new cloud service provider. And further, Service Level Agreements states that an Cloud Service Provider will not tamper or store your data for their use, so SLA's are one of the legal ways to protect data. But, this framework also protects the Data from residing on the Old cloud provider while it is being transmitted to the new cloud using the Hash algorithm included in the Cloud security framework.

5.4 Achievements

In the 2012 Cisco Global Cloud Networking Survey, over 1,300 IT professionals were surveyed about the challenges associated with cloud migration. The respondents named reliability, security and performance as the most difficult aspects of moving to the cloud. In fact,

almost 40 percent of respondents said they "would rather get a root canal, dig a ditch, do their own taxes" than have to orchestrate a cloud migration. And while cloud migration challenges do exist, having an experienced team behind you can make a big difference— and help ensure success. According to a recent article from the *International Organization of Scientific Research Journal*, the following are some of the main obstacles commonly associated with cloud migration. [91]

- **Sensitive data:** Organizations of all types base their operations on the cost of the data they store or share. But when they migrate to the cloud, all or part of that data is moved to the cloud server. This means that sensitive data is put at risk during the process of migration. If this data is leaked, companies can incur a large amount of damage, whether in terms of cost or reputation. Therefore, many business leaders feel that the hazards outweigh the benefits. However, with the right skills and experience, migration can be carried out in a safe way.
- **Data security:** It's common knowledge that the biggest issue in today's IT industry is internet security. Because of this, the process of migration must be carefully completed by experts. When data is moved from a physical server into the cloud, your company's data can be vulnerable. Therefore, it is so important to find and implement security solutions for sensitive information.
- **Interoperability:** This term refers to "the ability of systems to communicate" with one another, and it's one of the most pressing issues in cloud migration. When working within the cloud framework, 'communication' means something different than it usually does. It is the ability to write code that can work with multiple cloud providers at the same time, despite differences between them. Your cloud environment should be compatible with more than one cloud provider.

- **Portability:** Portability is "the ability to run components or systems written for one environment in another environment." To ensure portability, the software you want to migrate needs to be portable with other cloud environments.
- **Adoptability:** The challenge with implementing any new policy or system is the transition period. Your team has to learn a new process and adapt. Any time an organization adopts cloud computing, changes to "mission, authority, funding and staffing" will occur in various departments.
- **Cost and time:** Moving an existing workload to the cloud requires time and resources. This challenge is from a financial standpoint. Some of the specifics that are particularly important include the bandwidth cost of migration and the time it takes to transfer.

TABLE. 8

ADVANTAGES OF USING THE PROPOSED CLOUD MIGRATION FRAMEWORK

ISSUE	**RESOLVED STATUS**
Sensitive Data / Data Security	Resolved (Using Hash algorithm and Data logging framework integrated in Migration Framework)
Interoperability	Resolved (Platform Independency)
Portability	Resolved (It can be added as Desktop application or an Extension to Cloud Application)
Adoptability	Resolved (Easy to use)
Cost & Time	Resolved (Cost: Free, Time: Saves a lot)

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

The novel migration framework is exposed to be faster, as there is no such previous contribution in the field of cloud to cloud migration, we tried to compare our work with the traditional uploads and downloads of music files and with different formats too. While performing the simulation, we also had to consider some flaws like the interruption in the internet connections, server failure, low bandwidth and low frequency sometimes. But, the proposed framework resumes from the point where the data transfer was paused due to some interruptions in the internet.

As the results proved that the proposed framework is faster than the traditional transfer techniques, it has some advantages such as making the cloud portability possible, making the cloud a platform independent (irrespective of programming language used) it can be made compatible with any language platform, and finally faster data transfer with enhanced security features. We conclude that the proposed cloud migration framework solves the problem of cloud data migration and application lock ins with the concept of amazon Database migration, Tsunami protocol (combination of TCP and UDP) migration architecture, and cloud data logging framework, NetApp's NVRAM WAFL technologies. Comparing with the traditional transfer the migration framework takes 20% less time than the traditional.

6.2 Future Work

In future, we expect the framework to 15% more faster than the present one, and with enhanced two-layered security with biometrics (face scan, retina scan, finger-print access) in making the migration framework more secure.

REFERENCES

REFERENCES

[1]. "The GNU Operating System and the Free Software Movement", *Gnu.org*, 2017. [Online]. Available: http://www.gnu.org. [Accessed: 15- Mar- 2017].

[2]. Hassan, Qusay (2011). "Demystifying Cloud Computing" (PDF). The Journal of Defense Software Engineering. CrossTalk. 2011(Jan/Feb): 16–21. Accessed November 29, 2017.

[3]. Peter Mell and Timothy Grance (September 2011). The NIST Definition of Cloud Computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce. doi:10.6028/NIST.SP.800-145. Special publication 800-145.

[4]. M. Haghighat, S. Zonouz, & M. Abdel-Mottaleb (2015). CloudID: Trustworthy Cloud-based and Cross- Enterprise Biometric Identification. Expert Systems with Applications, 42(21), 7905–7916.

[5]. "What is Cloud Computing?". Amazon Web Services. 2013-03-19. Accessed November 29, 2017.

[6]. Baburajan, Rajani (2011-08-24). "The Rising Cloud Storage Market Opportunity Strengthens Vendors". It.tmcnet.com. Accessed November 29, 2017.

[7]. Oestreich, Ken, (2010-11-15). "Converged Infrastructure". CTO Forum. Thectoforum.com. Archived from the original on 2012-01-13. Accessed November 29, 2017.

[8]. "Where's The Rub: Cloud Computing's Hidden Costs". 2014-02-27. Accessed November 29, 2017.

[9]. “Cloud Computing: Clash of the clouds”. The Economist. 2009-10-15. Accessed November 29, 2017.

[10]. “Gartner Says Cloud Computing will be as influential as e-Business” Gartner. Accessed in November 14, 2017.

[11]. Gruman, Galen (2008-04-07). “What cloud computing really means”. InfoWorld. Accessed November 29, 2017.

[12]. Dealey, C. “Cloud Computing Working Group”, Network Centric Operations Industry Consortium - NCOIC, 2013

[13]. “The economy is flat so why are financials Cloud vendors growing at more than 90 percent per annum?”. FSN. Accessed November 29, 2017.

[14]. “Realization of Interoperability & Portability Among Open Clouds by Using Agent's Mobility & Intelligence - TechRepublic”. TechRepublic. Accessed November 29, 2017.

[15]. “Interoperability and Portability among Open Clouds Using FIPA Agent / 978-3-659-24863-4 / 9783659248634 / 3659248630”. www.lap-publishing.com. Accessed November 29, 2017.

[16]. Hassan, Qusay F.; Riad, laa M.; Hassan, Ahmed E. (2012). “Software reuse in the emerging cloud computing era”. In Yang, Hongji; Liu, Xiaodong. Understanding Cloud Computing (PDF). Hershey, PA: Information Science Reference. pp. 204–227. ISBN 978-1-4666-0897-9. doi:10.4018/978-1-4666-0897-9.ch009. Accessed November 29, 2017.

[17]. Schmidt, Eric; Rosenberg, Jonathan (2014). How Google Works. Grand Central Publishing. p. 11. ISBN 978-1-4555-6059-2.

[18]. “Internet History”, 2010. [Online]. Available: https://www/wikipedia.org. [Accessed: 06- Feb- 2015].

[19]. “National Science Foundation, “Diagram of CSNET,” 1981”.

[20]. White, J.E. “Network Specifications for Remote Job Entry and Remote Job Output Retrieval at UCSB”. tools.ietf.org. Accessed November 29, 2017.

[21]. “July 1993 meeting report from the IP over ATM working group of the IETF”. CH: Switch. Archived from the original on 2012-07-10. Accessed November 29, 2017.

[22]. Corbató, Fernando J. “An Experimental Time-Sharing System”. SJCC Proceedings. MIT. Accessed November 29, 2017.

[23]. Rochwerger, B.; Breitgand, D.; Levy, E.; Galis, A.; Nagin, K.; Llorente, I. M.; Montero, R.; Wolfsthal, Y.; Elmroth, E.; Caceres, J.; Ben-Yehuda, M.; Emmerich, W.; Galan, F. “The Reservoir model and architecture for open federated cloud computing”. IBM Journal of Research and Development. 53 (4): 4:1–4:11. doi:10.1147/JRD.2009.5429058.

[24]. Kyriazis, D; A Menychtas; G Kousiouris; K Oberle; T Voith; M Boniface; E Oliveros; T Cucinotta; S Berger (November 2010). “A Real-time Service Oriented Infrastructure”. International Conference on Real-Time and Embedded Systems (RTES 2010). Singapore.

[25]. Gogouvitis, Spyridon; Konstanteli, Kleopatra; Waldschmidt, Stefan; Kousiouris, George; Katsaros, Gregory; Menychtas, Andreas; Kyriazis, Dimosthenis; Varvarigou, Theodora (2012). “Workflow management for soft real-time interactive applications in virtualized environments”. Future Generation Computer Systems. 28 (1): 193–209. ISSN 0167-739X. doi: 10.1016/j.future. November 29, 2017.

[26]. Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, citing the Gartner report, “Cloud Computing Confusion Leads to Opportunity”. Accessed November 29, 2017.

[27]. Gartner (November 29, 2017). “Gartner Says Worldwide IT Spending on Pace to Surpass Trillion in 2008”.

[28]. “Announcing Amazon Elastic Compute Cloud (Amazon EC2) - beta”. Amazon.com. 24 August 2006. Accessed November 29, 2017.

[29]. “Windows Azure General Availability”. The Official Microsoft Blog. Microsoft. 2010-02-01. Accessed November 29, 2017.

[30]. DZone, “Apache CloudStack vs. OpenStack: Which Is the Best?”, https://dzone.com/articles/apache-cloudstack-vs-openstack-which-is-the-best Accessed November 29, 2017.

[31]. Software Insider, “OpenNebula vs OpenStack”, http://cloud-computing.softwareinsider.com/compare/70-322/OpenNebula-Project-vs-OpenStack-Foundation Accessed November 29, 2017.

[32]. Kostantos, Konstantinos, et al. “OPEN-source IaaS fit for purpose: a comparison between OpenNebula and OpenStack.” International Journal of Electronic Business Management. Accessed November 29, 2017.

[33]. L. Albertson, “OpenStack vs. Ganeti”, Linux Fest Northwest 2017.

[34]. Qevani, Elton, et al. “What can OpenStack adopt from a Ganeti-based open-source IaaS?” Cloud Computing (CLOUD), IEEE 7th International Conference on. IEEE, 2014.

[35]. Von Laszewski, Gregor, et al. “Comparison of multiple cloud frameworks.”, IEEE 5th International Conference on Cloud Computing (CLOUD), 2012.

[36]. Diaz, Javier et al. “Abstract Image Management and Universal Image Registration for Cloud and HPC Infrastructures “, IEEE 5th International Conference on Cloud Computing (CLOUD), 2012.

[37]. “Launch of IBM Smarter Computing”. Archived from the original on 20 April 2013. Accessed November 29, 2017.

[38]. “Launch of Oracle Cloud”. Accessed November 29, 2017.

[39]. “Oracle Cloud, Enterprise-Grade Cloud Solutions: SaaS, PaaS, and IaaS”. Accessed November 29, 2017.

[40]. “Larry Ellison Doesn't Get the Cloud: The Dumbest Idea of 2013”. Forbes.com. Accessed November 29, 2017.

[41]. “Oracle Disrupts Cloud Industry with End-to-End.

[42]. “Introducing Google App Engine + our new blog”. Google Developer Blog. 2008-04-07. Accessed November 29, 2017.

[43]. “Google Compute Engine is now Generally Available with expanded OS support, transparent maintenance, and lower prices”. Google Developers Blog. 2013-12-02. Accessed November 29, 2017.

[44]. HAMDAQA, Mohammad (2012). Cloud Computing Uncovered: A Research Landscape (PDF). Elsevier Press. pp. 41–85. ISBN 0-12-396535-7.

[45]. “Distributed Application Architecture” (PDF). Sun Microsystem. Accessed November 29, 2017.

[46]. Skala, Karolj; Davidović, Davor; Afgan, Enis; Sović, Ivan; Šojat, Zorislav (2015-12-31). “Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing”. Open Journal of Cloud Computing. RobPub. 2 (1): 16–24. ISSN 2199-1987.

[47]. “It's probable that you've misunderstood 'Cloud Computing' until now”. TechPluto. Accessed 2010-09-14.

[48]. Danielson, Krissi “Distinguishing Cloud Computing from Utility Computing”. Ebizq.net. Accessed November 29, 2017.

[49]. “Recession Is Good for Cloud Computing – Microsoft Agrees”. Cloud Ave. Accessed November 29, 2017.

[50]. “Defining 'Cloud Services' and “Cloud Computing”“. IDC. 2008-09-23. Accessed November 29, 2017.

[51]. “e-FISCAL project state of the art Repository”. Accessed November 29, 2017.

[52]. Farber, Dan (2008-06-25). “The new geek chic: Data centers”. CNET News. Accessed November 29, 2017.

[53]. “Risky Bet on Clouds”, 2016. [Online]. Available: http://www.amazon.com/cloud. [Accessed: 06- Feb- 2016].

[54]. He, Sijin; Guo, L.; Guo, Y.; Ghanem, M. “Improving Resource Utilization in the Cloud Environment Using Multivariate Probabilistic Models”. 2012 2012 IEEE 5th International Conference on Cloud Computing (CLOUD): 574–581. ISBN 978-1-4673-2892-0. doi:10.1109/CLOUD.2012.66.

[55]. He, Qiang, et al. “Formulating Cost-Effective Monitoring Strategies for Service-based Systems Accessed November 29, 2017.

[56]. A Self-adaptive hierarchical monitoring mechanism for Clouds Elsevier Accessed November 9, 2016.

[57]. Heather Smith (23 May 2013). Xero For Dummies. John Wiley & Sons. pp. 37–. ISBN 978-1-118-57252-8.

[58]. King, Rachael (2008-08-04). “Cloud Computing: Small Companies Take Flight”. Bloomberg BusinessWeek. Accessed November 29, 2017.

[59]. Mao, Ming; M. Humphrey (2012). “A Performance Study on the VM Startup Time in the Cloud”. Proceedings of 2012 IEEE 5th International Conference on Cloud Computing (Cloud2012): 423. ISBN 978-1-4673-2892-0. doi:10.1109/CLOUD. Accessed November 29, 2017.

[60]. Dario Bruneo, Salvatore Distefano, Francesco Longo, Antonio Puliafito, Marco Scarpa: Workload-Based Software Rejuvenation in Cloud Systems. IEEE Trans. Computers 62(6): 1072–1085 (2013).

[61]. “Defining and Measuring Cloud Elasticity”. KIT Software Quality Department. Accessed August 13, 2017.

[62]. “Economies of Cloud Scale Infrastructure”. Cloud Slam 2011. Accessed November 27, 2017.

[63]. He, Sijin; L. Guo; Y. Guo; C. Wu; M. Ghanem; R. Han. “Elastic Application Container: A Lightweight Approach for Cloud Resource Provisioning”. 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (AINA): 15–22. ISBN 978-1-4673-0714-7. doi:10.1109/AINA.2012.74.

[64]. Marston, Sean; Li, Zhi; Bandyopadhyay, Subhajyoti; Zhang, Juheng; Ghalsasi, Anand (2011-04-01). “Cloud computing – The business perspective”. Decision Support Systems. 51 (1): 176–189. doi: 10.1016/j.dss. Accessed August 13, 2017.

[65]. Mills, Elinor (2009-01-27). “Cloud computing security forecast: Clear skies”. CNET News. Accessed August 13, 2017.

[66]. Duan, Yucong; Fu, Guohua; Zhou, Nianjun; Sun, Xiaobing; Narendra, Nanjangud; Hu, Bo. “Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends”. IEEE. Accessed January 15, 2017.

[67]. Kurdi, Heba; Li, Maozhen; Al-Raweshidy, H. S. (2010). “Taxonomy of Grid Systems”. In Antonopoulos, Nick. Handbook of Research on P2P and Grid Systems for Service-Oriented Computing: Models, Methodologies and Applications. IGI Global research collection. IGI Global. p. 34. ISBN 978-1-61520-687-2. Accessed 2015-07-29. Nowadays Service-Oriented Architecture (SOA) has become as [sic] the main architectural model of many IT initiatives including grid, cloud and everything as a service (Essa\XaaS\aas) computing.

[68]. Alcaraz Calero, Jose M.; König, Benjamin; Kirschnick, Johannes (2012). “Cross-Layer Monitoring in Cloud Computing”. In Rashvand, Habib F.; Kavian, Yousef S. Using Cross-Layer Techniques for Communication Systems. Premier reference source. IGI Global. p. 329. ISBN 978-1-4666-0961-7. Accessed November 29, 2017. Cloud Computing provides services on a stack composed of three service layers (Hurwitz, Bloor, Kaufman, & Halper, 2009): Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

[69]. “Cloud is Emerging”, *Synergy Creative Solutions*, 2017. [Online]. Available: http://www.synergycreativesolutions.com/cloudblog. [Accessed: 06- Feb- 2017].

[70]. Understanding Cloud Computing Vulnerabilities Grobauer,B.; Walloschek, T.; IEEE Volume: 9, Issue: 2 Digital Object Identifier: 10.1109/MSP.2010.115 Publication Year: 2011, Page(s): 50-57.

[71]. Comparison of several cloud computing platforms Junjie Peng; Xuejun Zhang; Zhou Lei; Bofeng Zhang; Wu Zhang; Qing Li; Information Science and Engineering (ISISE), 2009 Second International Symposium on Digital Object Identifier: 10.1109/ISISE.2009.94 Publication Year: 2009, Page(s): 23 – 27.

[72]. Cloud Storage as the Infrastructure of cloud computing Jiyi Wu; Lingdi Ping; Xiaoping Ge; Ya Wang; Jianqing Fu; Intelligent Computing and Cognitive Informatics (ICICCI), 2010 International Conference on Digital Object Identifier: 10.1109/ICICCI.2010.119 Publication Year: 2010, Page(s): 380 – 383.

[73]. The characteristics of cloud computing Chunye Gong; Jie Liu; Qiang Zhang; Haitao Chen; Zhenghu Gong; Parallel Processing Workshops (ICPPW), 2010 39th International Conference on Digital Object Identifier: 10.1109/ICPPW.2010.45 Publication Year: 2010, Page(s): 275 – 279.

[74]. Furfaro, A.; Garro, A.; Tundis, A. (2014-10-01). "Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing". 2014 International Carnahan Conference on Security Technology (ICCST): 1–6. doi:10.1109/CCST.2014.6986995.

[75]. "SeaaS - TechTarget", *TechTarget*, 2017. [Online]. Available: http://www.techtarget.com. [Accessed: 06- Feb- 2016].

[76]. Carney, Michael. "Any Presence partners with Heroku to beef up its enterprise MBaaS offering". Pando Daily. Accessed 24 June2013.

[77]. Alex Williams (11 October 2012). "Kii Cloud Opens Doors for Mobile Developer Platform With 25 Million End Users". TechCrunch. Accessed November 29, 2017.

[78]. Aaron Tan (30 September 2012). "Fat Fractal ups the ante in backend-as-a-service market". Techgoondu.com. Accessed November 29, 2017.

[79]. Dan Rowinski (9 November 2011). "Mobile Backend as A Service Parse Raises $5.5 Million in Series A Funding". Read Write. Accessed 23 October 2017.

[80]. Pankaj Mishra (7 January 2014). "MobStac Raises $2 Million in Series B To Help Brands Leverage Mobile Commerce". TechCrunch. Accessed 22 May 2017.

[81]. "Built.io Is Building an Enterprise MBaaS Platform for IoT". Programmable web. Accessed 3 March 2014.

[82]. Miller, Ron (24 Nov 2015). "AWS Lambda Makes Serverless Applications A Reality". TechCrunch. Accessed November 29, 2017.

[83]. "Cloud Deployment Models", *Whatiscloud.com*, 2017. [Online]. Available: http://whatiscloud.com/cloud_deployment_models. [Accessed: 06- Jan- 2017].

[84]. "Cloud Computing Trends: 2017 State of the Cloud Survey", *Rightscale.com*, 2017. [Online]. Available: https://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey. [Accessed: 06- Feb- 2017].

[85]. Marsh. Donna, "How to Keep a Home Phone Number", *It Still Works | Giving Old Tech a New Life*, 2009. [Online]. Available: http://www.ehow.com/how_4850788_keep-home-phone-number.html. [Accessed: 08- Apr- 2017].

[86]. "Database Migration: An in-Depth look!! (Level 400 Session)", Developeriq.in, 2008. [Online]. Available: http://developeriq.in/articles/2008/may/09/database-migration-an-in-depth-look-level-400-sess/. [Accessed: 19- Apr- 2017].

[87]. Service Migration in Cloud Architecture Kaisler, S.; Money, W.H.; System Sciences (HICSS), 2011 44th Hawaii International Conference on Digital Object Identifier: 10.1109/HICSS.2011.371 Publication Year: 2011, Page(s): 1 – 10.

[88]. R. Buyya, C. Yeo and S. Venugopal "Market oriented cloud computing: Vision, hype and reality for delivering it services as utilities," in proceedings of 10th IEEE conference Accessed January 15, 2017.

[89]. Jainish Rajesh Jain and Dr. Abu Assaduzaman "Secure Data Logging Framework to enhance security in cloud" IEEE SouthEastCon 2016.

[90]. "Tsunami UDP Protocol – Installation, Setup and Limitations", Bluepiit.com, 2015. [Online]. Available: https://www.bluepiit.com/blog/tsunami-udp-protocol-installation-setup-and-limitations/. [Accessed: 06- Jan- 2017].

[91]. Jonathan. Jones." Biggest Cloud Migration Challenges", 21st July 2015. [Online]. Available: https://www.glowtouch.com/blog/cloud/what-are-the-biggest-challenges-that-occur-with-cloud-migration/. Accessed: August 21, 2017.