International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 11, Issue 6, June 2020, pp. 264-280, Article ID: IJARET_11_06_024
Available online athttp://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=6
ISSN Print: 0976-6480 and ISSN Online: 0976-6499
DOI: 10.34218/IJARET.11.6.2020.024

A FRAMEWORK FOR IMPROVING INFORMATION SECURITY USING CLOUD COMPUTING

Wasan S. Awad
Ahlia University, Bahrain

ABSTRACT

The main objective of this paper is to propose a cloud based framework handling security issues in the existing data storage systems. There are various cyber security threats to existing storage systems because of their traditional architecture and operations applied on them for managing the data within Bahrain. Migration of local storage services to cloud environment is found to solve numerous related cyber security issues within Bahrain. On the other hand, a number of cyber security vulnerabilities are found to be emerged as a result of this migration such as public networks exposure and multitenant shared infrastructure. The vulnerabilities due to this transition introduce the security breaches and hence cause a threat to the underlying confidential information. The significance of migrating storage services to the cloud environment and the emerging cyber security issues in such a transition are analyzed thoroughly. The proposed framework is intended to support the existing information systems security schemes. It also provides the cyber security professionals with the ability to design, and customize cloud services that better suits the needs of organizations.

Key words: cyber security, threats, attacks, risk assessment, cloud computing, Storage systems

Cite this Article: Wasan S. Awad, A Framework for Improving Information Security Using Cloud Computing, *International Journal of Advanced Research in Engineering and Technology*, 11(6), 2020, pp. 264-280.
http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=6

1. INTRODUCTION

Storage systems are of high importance for every organization. It caters all the confidential and valuable information about a certain organization. Moreover, the organizational data keeps on incrementing exponentially and scalability of their storage systems are always desired. By doing so, effective management of the valuable information is made possible. Hence the storage is managed using different applications and architectural models. There are various kinds of storage systems and the decision of choosing a particular storage system over another for a specific application to manage the system depends on a lot of factors. One of

them is the growing number of cyber attacks and the need of relevant cyber security measures that is the main focus of this research.

Cyber security is becoming a major issue worldwide and is a highest level agenda of the top decision makers. Thus, the security of important systems that affects the performance of the organizations should be assessed and improved. Storage systems are the ones that can potentially suffer lots of breaches and most vulnerable in many of the organizations. Securing these storage systems are highly important tasks to maintain confidentiality and integrity of data within an organization. Some of those vulnerabilities are lack of access control, weak password policies and ineffective firewall protocols.

Securing local storage systems can be improved by using two approaches. First is the traditional approach comprising of certain techniques that are costly for an organization and add more processing load on the available infrastructure while reducing the overall performance. This may need upgrades to remove such performance related problems while retaining the security of the system. The second approach is based on cloud computing that reduces the performance overhead. Some IT professionals believes in cloud as an enhancement to the cyber security paradigm while others are on countering the notion by believing that cloud deteriorate cyber security models. In this paper, using cloud storage services instead of the traditional storage server is studied from cyber security point of view.

2. RESEARCH OBJECTIVES

The main objective of this paper is to propose a cloud based framework to improve the security of storage systems for Bahraini organizations that are possessing limited resources. Thus, this paper is to answer the following questions regarding the cyber security of the current storage system and cloud storage services:

- Will migrating to cloud services solve the current challenges with current systems?
- What are the security threats that are attached to the transition from locally hosted to cloud services?
- What are the security techniques that can mitigate these threats?
- How the security techniques can be integrated in a secure system design for cloud computing services?

The proposed solution is a transition from the current storage server located on the local network to the storage services available remotely on the cloud. These services are provided by different vendors that are specifically tailored to the needs of the enterprises. The transition will introduce new security risks and challenges that are also analyzed in this study.

3. RESEARCH METHODOLOGY

To answer the research questions, the assessment of the security of local (current) storage system is required. The assessments that has been conducted is qualitative assessment due to the fact that quantifying the impact of cyber security breaches is a huge exercise that requires dedication from a lot of personnel from the organization under assessment because the value of information and the value impact of a security breach is not a straight forward number that is available in the organization. Qualitative values of the impacts are based on literature and research available on storage systems. For the assessment plan, a risk matrix have been identified and utilized for the risk ratings based on the impact and probability. Note that, impact and probability are also referred to as consequence and likelihood in literature. The general trend of risk matrices follows the theorem which states that the risk increases when any one of the two arms consequence and likelihood increase. The security assessment has been carried out in the storage security domains:

- Application access domain.
- Management access domain.
- Backup, replication and archive domain.

Awad and Abdullah (2014) proposed a risk assessment model for cyber security of local storage systems. The model is based on risk matrix and was implemented for two organizations in Bahrain. The risk assessment results have shown security risks of different ratings in the local storage systems of the assessed organizations. Risks have been identified, and security techniques required to mitigate the identified risks have been discussed. It has been found that application of those techniques and the rapid evolution of cyber attacks impose high demand of resources overhead on the organizations.

The results of the risk assessment of local storage systems show the existence of weaknesses and vulnerabilities in them, specifically when there is no dedicated staff to look after the security issues in those storage systems. These weak security aspects of the storage systems in the two Bahraini organizations can be classified into personal, technical, and strategic:

Personal: There are no dedicated personnel for the security of storage. There are no clear separations of privileges such as power users that have different levels of administrative roles compared to the administrator accounts with full privileges of all administrative tasks. Moreover, the governing part of cyber security is handled by the same entity responsible for its implementation.

Technical: There is no centralized continuously monitored security logging system that aggregates all of the different security logs from the storage infrastructure devices. Moreover, there is no encryption while transiting over the different components of the storage infrastructure. Apart from that, there is no dedicated integrity assurance/firewall service for the storage system. The ports on the network are not checked regularly to block any unused ports. There is no remote disaster recovery site maintained, even the backups are not encrypted and have no authentication requirement for restoration.

Strategic: The organizations do not benchmark its cyber security framework against comparatives. There is no disaster recovery plan or business continuity management procedure Moreover, there is no data retention policy and procedure.

In this research, using the cloud storage services as an alternative technique is investigated. In addition, the security effects in particular of such a transition are studied. The first part of this study is about how this transition will affect the current threats of the local storage systems, and the second part is the new security risks which will be introduced because of this transition. Finally a whole secure cloud storage system framework is proposed based on security techniques to mitigate the introduced security threats.

4. LITERATURE REVIEW

The following subsections are providing the relevant insight of existing techniques in the domain of cloud computing and its security.

4.1. Cloud Computing

Cloud computing refers to the information technology model of providing computing resources and services such as networks, servers, storage, applications, or service through any type or size of computer network or the internet (Antono poulos and Gillam, 2010).

Cloud models are differentiated based on service purpose, capacity and security requirements. Deployment model and service model are two characteristics that identify a lot of specifications of the cloud based infrastructure. There is several deployment models

defined in literature. Deployment model reflects the management, service delivery and customer class characteristics of a cloud service. The following are the most common models as defined by (Hurwitz and Kaufman, 2011; Jansen and Grance, 2011;Hurwitzand Kaufman, 2011):

- Public Cloud
- Private Cloud
- Community Clou
- Hybrid Cloud

Service model is another key characteristic of cloud. Service models are independent from deployment models. In other words, each service model can be provided using any deployment model. The following are the basic service models used in the cloud industry (Dawoud, Takouna, andMeinel, 2010; Gibson, et al. 2012; Maddineni, and Ragi, 2011):

- Software-as-a-Service (SaaS)
- Platform-as-a-Service (PaaS
- Infrastructure-as-a-Service (IaaS)

4.2. Cloud Computing Characteristics

Any decision maker in an organization needs to understand a new technology from all of its aspects before taking a decision in the feasibility of acquiring the technology to the organization. Migrating to cloud computing is such a big decision and strategic movement that requires high attention to benefits and drawbacks of such a change (Gibson, et al., 2012).

Benefits: The following are the major benefits of cloud computing(Bhardwaj and Kumar, 2011; Bhisikar, and Sahu, 2013;Gibson, et al., 2012;MellandGrance, 2011; Sadiku, Musa, and Momoh, 2014).

- Cost: Cost is the most apparent and clear benefit from using cloud computing services. Obviously there will be cost elimination of Hardware, Software, upgrades, maintenance staff, spares, licenses, support contracts, and environment utilities etc.
- Efficiency: In cloud computing a consumer estimates exactly how many resources required for the applications and set the service contract on that basis.
- Flexibility: Upgrades and bottle nicking of in-house installations is not easy and the time it requires is not predictable. On the other hand, cloud computing is a modular service that is easily expandable and resources are always available for any kind of application.
- Availability: Assuming that the communication channel is reliable and have all the means of redundancy and resilience, the availability of cloud services is better than the availability of in-house systems because of the large scale system that have bullet proof protection, recovery, monitoring and maintenance capabilities.
- Environmental Friendly Solution: Utilizing cloud computing is a “Green” step because of couple of reasons.
- Security: Cloud computing has significant security advantages in addition to the drawbacks that it brings.

Drawbacks: The disadvantages of cloud computing are very well elaborated by (Bhardwaj and Kumar, 2011; Bhisikar, and Sahu, 2013; Sadiku, Musa, and Momoh, 2014) as following.

- Control: A decision maker with a confidentiality oriented mind will never allow a step towards cloud computing because eventually not only the data of the organization is

out of the premises of it but also the control over the infrastructure that provides the service.

- Performance: Performance is not a clear cut disadvantage of cloud computing although there are enabling features that increases the possibilities of having deficiencies in performance.
- Reliability: Reliability is dependent on the cloud service provider. Cloud service providers vary in managing performance, availability and control issues. All of which affects the reliability level of the service.
- Bandwidth Cost: Bandwidth cost in still an issue that depends on two factors. The first factor is the intense of the data being transferred over the communication channel. The second factor is the type of channel required that is dependent on the confidentiality and reliability level.
- Security: It is quite interesting that security is listed in the advantage sand the disadvantages sections and that is because of the wide range of aspects and varied domain that is considered to be the cyber security domain.

It is very much clear that all of the issues whether an advantage or a drawback depends on how service providers deal with it and act upon.

4.3. Related Work

Organizations and companies tends to concentrate on the core business they perform and that is why they have a habit of subcontracting any service that is not in the core business specially if subcontracting the job do not affect the performance and the efficiency and the cost as well.

A lot of the work related to IT stuff has been subcontracted from a very long time but always the subcontractor mobilizes to the organization perimeter and work on their system. When cloud services came into the picture the domain of subcontracting has been widened and the whole service and infrastructure has been subjected to subcontracting (Meetei, 2013). A lot of organizations were reluctant to do so at the beginning similar to any new technology and specially the performance, efficiency and security were all topics that is still does not give a strong confidence for a transition to cloud. In the latest years and as the technology enhances and introduced positively in front of the public and private sector, different companies has at least migrated some of its services to the cloud. At the same time, a lot of critical industries and confidential organizations have not taken such a step (Rao and Sarathy, 2009).

It is very obvious after going through a tremendous number of literatures that most of the questions and doubts have answers, and different options are available for different categories of organizations within the domain of cloud services technologies.

Cloud is one of the approaches used to implement storage systems that have been studied by many researchers while presenting cloud technology as networks of the future, such as, Ramachandran, (2018) who proposed a new cloud software engineering process, architecture, and techniques that can be used to develop reliable, flexible, and reusable computing systems. Other researchers introduced, analyzed and presented a robust research covering well established cloud providers that are offering cloud services to the public. For the reason of computing capability when utilizing cloud computing as a technology, researchers suggested cloud as being a major step in the computing spectrum and performance (Bhisikar and Sahu, 2013; Hutchison2011;Mollah,Islam, and Islam, 2012; Zhou, et al., 2010). Furthermore, cloud security has been investigated by a number of researchers. Some researchers (Suganya and Damodharan, 2013;Wang, et al., 2009; Mahmood, Z. and Saeed, S., 2013) have presented

certain methodologies to enhance and fill gaps in the cyber security models of storage services offered by cloud providers.

In (2012), Liu announced some cloud computing systems, and investigated cloud computing security issues and its approaches according to the cloud computing features and concepts. Also, he illustrated a cloud conception and verified the cloud abilities such as scalability, elasticity, platform independent, low-cost and reliability

5. PROPOSED FRAMEWORK FOR SECURED CLOUD BASED STORAGE SYSTEM

This section analyzes and elaborates the security aspects and potential vulnerabilities of cloud based storage services. Furthermore, storage security proposal and cloud migration proposal provides an insight of relevant vulnerabilities and security strengths in cloud based storage. Based on the analyzed vulnerabilities, the framework for securing cloud storage systems is proposed.

Storage cloud is IaaS that gives consumer organizations a sufficient level of scalability and flexibility in using the virtualized environment for its storage requirements. IaaS is the foundational level for other models and services (Dawoud, Takouna, and Meinel, 2010).Cloud service providers costs the consumer three main categories of payments for storage services. Pre-operation charges that are fixed normally and kits value depends heavily on the requirements of the consumer that is negotiated in the service contract formation stage.

The other two categories of payment are variables and dependent on the amount of storage capacity required and the bandwidth required. In most of the cases, the first requirement which is the storage capacity has different classes of payments that are dependent on the capacity. In other words, the cost of one GB when the whole requirement does not exceed one TB is different from the cost one GB when the total requirement exceeds one TB (Bilski, 2007).

The second variable cost is the bandwidth cost and that has also different rates for upload and downloads in most of the cases. In addition, part of the IaaS package is computational resources. This computational resource allows consumer users to use data stored without the need for download or upload.

Cloud storage services are very attractive and allow consumers to transfer a lot of their applications that are storage centric such as email systems, communication tools, data sharing and backup and restore management (Kumar, et al., 2012).

5.1. Migrating Storage to Cloud

The benefits and feasibility of transferring to cloud that is summarized in the question “Why transferring to cloud?” is not a doubtful topic anymore. Instead, the topic that is doubtful and pops up a lot of discussions nowadays is “How to migrate to cloud?” and “How to transfer services to cloud?”

There are different approaches to migrate storage services and data from local systems to cloud infrastructure. All are dependent on the service provider, amount of data and systems, and security. There are even nowadays software packages that are specialized in migrating from one cloud to another. In general there are some guidelines that are always true in any migration plan for storage services(Koletka and Hutchison, 2011;Mathur and Nishchal, 2010):

- A migration plan should be developed carefully along with service provider and experts from the consumer side. If required, third party consultants should be hired to represent the consumer.

- In-house efforts should be made to catalog all storage requirements. Architecture drawings and systems inventories should be developed.
- In conjunction with the previous activity of inventorying and information gathering, a structure for authorizations and responsibilities should be developed to utilize the permissions and authorization features provided by cloud service provider.
- The files upload or transfer activity should be planned. Planning this activity should take into account the availability of the services which may lead to the utilization of non-business hours. If there are no non-business hours, which are the case for a lot of different ranges of businesses, an online or on-process migration should be planned.
- The migration plan should take into consideration securing the data during the transfer.
- After having the storage data on the cloud service provider facility, handing over responsibilities between the local storage systems and the cloud storage infrastructure should be planned.
- The operation after the migration should be tested and have a pilot period to ensure safe, secure and optimum performance.
- Remediation should be applied to any issue happens during the testing period. Excellent logging system is required to capture issues before affecting business.

Although cloud services may be foreseen as a solution to enhance the cyber security paradigm of the IT services an organization has, because the cloud service provider is a dedicated entity whose only business is to manage data centers and provide different levels of cloud services, cloud presents tremendous number of cyber security risk that are directly related to the use of cloud instead of having the services locally hosted. A recent survey shows that more than 80% of IT professionals believe that the biggest challenge with regards to cloud computing is security. Another study shows that in an enterprise of 5000 employees, the cost of security labor and productivity has dropped by 41% equivalent to 49$ per employee per year (Behl, 2011).

Cyber security benefits of transforming to cloud are discussed followed by the downsides from cyber security aspect of the transformation. The benefits of transforming to cloud are:

- Staff specialization: Similar to any other proficiency, IT organization size depends on the amount of work and scale of responsibilities. When the manpower is big, specialization comes into picture because there is a potential that allows doing so. For example, when accountancy responsibilities are of high scale such as in banking institutes an accountant have a lot of different specialized tracks to work in. In comparison, in another organization one or two accountants may do everything related to this domain without having specialty into a specific track. Cloud service providers for IT personnel are like banks for accountants, and security is one of the tracks that have a specialized staff that works only on cyber security full time. On the other hand as seen in the assessment, other organizations have IT personnel that does everything including security.
- Resource availability: Although availability enhancement in migrating to cloud may be challenged with the fact that the resources will be available through a multistage communication means and the resource availability is affected by the availability of the communication mean, availability can be enhanced by looking into the matter from different angle. Infrastructures of cloud providers have design redundancy, recovery and protection capabilities that reduce the possibility of having downtime to a very small fraction of the probability of in-house systems. In addition, when the traffic is

high and resources are being acquired by users in a very high scale in some occasions, cloud providers will have the resources mean to withstand in such situations although it might cost the customer depends on the contract agreement terms and conditions. In similar cases and when in-house systems do not manage to absorb the demand, systems may fail (Mathur and Nishchal, 2010).

- Backup and recovery: It is obvious from the assessment done on the governmental organizations that they do lack in backup mechanisms specially in the availability of offsite emergency or data recovery center (Awad and Abdullah, 2014). Cloud service providers have very robust backup and recovery capabilities and these capabilities are due to the fact that cloud providers cannot withstand a failure in their service to maintain quality and customer satisfaction.
- Remote users: In organizations that have IT systems onboard and do not use cloud services, an employee who needs to access organizational data on the go either take a copy of the data on the mobile device or have a remote connection to the organization systems. Both methods are dangerous and impose security threat because a mobile device may be stolen and as explained remote access security measures wouldn't be robust. In cloud computing, consumer is always in a remote condition whether in the company premises or not and securing the communication channel is a priority(Hurwitz and Kaufman, 2011).
- Data concentration: Because of the homogenous nature of systems structure in cloud data centers, a central storage system concentrates all of the data of a certain entity whereas in in-house based installation mostly data are scattered among systems and users (Hurwitz and Kaufman, 2011).

Some popular and common security issues and drawbacks that are introduced from migrating to cloud are:

- Shared multi-tenant environment: In most of the cases the cloud services provider serves multiple consumers and the resources available for consumers are separated logically rather than having physical separation. Such logical separation poses cyber security threat but is part of the integral idea and philosophy of cloud computing (Dinadayalan, et al., 2014).An intruder may utilize the access given to him as a consumer and find out a way to overcome the logical boundaries available to attack certain entity that utilizes the same cloud service.
- Public networks exposed services: Before having cloud services, all IT services were hosted internally in the organization and protected by the physical means of organizational physical security. Cloud services are hosted in a remote location from the organization and have a communication channel that communicates the services and data back and forth between the service provider and the consumer. The communication channel have a variety of fashions, some utilizes the internet which imposes very high risk due to the wide exposure surface (Muppala, et al., 2011). Others use telecommunication utilities infrastructures for dedicated communication channels. In some rare cases, consumer has a dedicated self-owned communication line all the way to the service provider. Security is availability and integrity as well and those factors may also deteriorate when a public communication channel is utilized. The last security drawback related to exposure to public networks is that in some cases and in addition to the data access, administrative access is also exposed as well.
- Loss of Control: Although cloud providers have highly specialized staff that may not be possible to mobilize by organization in-house, but the application of all security

policies and procedures is under the control of cloud provider (Sharma, et al., 2013). This makes a lot of security aspects vague for the consumer organization such as compliance, incident response, accountability and everything that is affected by losing the direct control.

5.2. Security Proposal

Organizations are recommended to consider the option of migrating storage services to cloud but with several precautions and advices that should be followed strictly in order to avoid making a strategic mistake instead of making a strategic move to the future.

The following is a summary of conclusions and recommendations that is followed by an elaboration of the proposal of consideration.

- The cyber security assessment has been conducted for two prestigious governmental organizations (Awad and Abdullah, 2014). It is believed that the results apply on a wide spectrum of governmental, semi-governmental and private sector corporations. These believe is supported by statistics that leads to the same conclusion.
- The results of the assessment have shown major discrepancies in the cyber security paradigm of the two organizations. If sustained, these cyber security discrepancies will lead to breaches in confidentiality, integrity or availability of information resources.
- Mitigating such discrepancies is possible by applying a number of suitable security techniques. Other organizations may require more or less mitigations depends on the shape of their cyber security paradigm.
- The mitigations required costs organizations of Bahrain a huge number of resources in terms of manpower, capital expenditure cost of projects and continue operations cost. Taking into consideration that cyber security is a very rapid evolving topic and the security model that is suitable for today is not definite to be suitable for tomorrow, costs will keep increasing. Organizational management requests their IT personnel to consider alternative solutions.
- The alternative solution that is discussed and proposed in this paper is the utilization of cloud computing. Although cloud has been widely used recently, but the idea of subcontracting supporting services that are not the core business of an organization is a very old strategy for businesses and organizations (Wang, et al., 2009).
- In the organization of Bahrain, it was obvious that they were welling to subcontract IT projects and operations requirement. Going into cloud is a further step into which the whole IT service is sub contracted.
- Before going into details of the cloud solution, cyber security should be evaluated. Advantages and disadvantages in addition to the ability to solve the current cyber security issues and keep a well maintained up to date security model should be presented for the case studied in this paper.
- All cyber security techniques in cloud computing is applied and most of the data centers that provides cloud computing services will have solutions that covers all of the security issues found in the assessment.
- Studying effect on existing cyber security issues when migrating to cloud is half of the picture only. In order to have the whole picture clear, introduced cyber security issues that is related to the nature of the cloud services should be assessed for the organizations of Bahrain to migrate to cloud safely and with convince.
- Cyber security introduced issues such as exposure to public networks and loss of control. These issues have mitigations as well. It all depends on the cloud service

provider for which the methodology for selecting the provider is important. Thus, the recommendation is to form a governmental cloud company that uses the community service model for governmental institutes and provides IaaS for storage services as a deployment model.

- Based on our previous study (Awad and Abdullah, 2014), organizations in Bahrain should be convinced of the cyber security benefits they will have from migrating to cloud service following the service model and deployment model suggested here. There are certain things to be considered in migration to cloud as will be shown later.

5.3. Cloud Migration Proposal

Organizations must follow the following steps in considering cloud services:

- Analyze organizational requirement for IT services and cloud services specifically.
- Apply international codes, standards, and guidelines.
- Assess, select, engage and later oversee the cloud service that best suit the requirement.

National Institute of Standards and Technology (NIST) (Mell and Grance, 2011), European Telecommunication Standards Institute (ETSI), and International Telecommunication Union (ITU) are examples of prestigious international standardization organizations that have published standards for different aspects of cloud computing.

Normally cloud services are considered to achieve certain goals that mainly revolve around two points: cost reduction and efficiency growth. Security is supposed to be an area where compromises will take place in favor of cost and efficiency. At the same time, due to the rapid and heavy increase in cyber security risks, cyber security systems have evolved (Leavitt, 2009). In order to achieve security in systems that are maintained locally, an organizational line should be established and a lot of efforts, cost and procedures should be taken place which may deviates the organization from its goals.

Except for the fact that the data is in other organizational premises and communication means are required, it is found that security enhances positively by migrating storage services to cloud because of the lack of ability to catch the evolution in cyber security risks and technologies and the requirements for that in-house (Kumar, et. al., 2012; Jiunn-Woei, et. al., 2014)).On the other hand, and as stated earlier cloud introduces new cyber security threats that should be addressed and tackled in the right way in order to get all of the benefits of cloud without compromising security and this is addressed in the following major recommendations of this proposal:

Addressing cloud computing risks: The consumer should form a task force for risk management to deal with cyber security risks associated to the utilization of cloud services. This task force will have inputs to the service contract components required (Bensoussan and SingRu, 2011).

Servicing data center location: One of the most important recommendations related to the service is the knowledge of the location of the data and applications. Some cloud providers have datacenters in different countries and the services provided for a consumer including the storage service may be provided by resources of more than one data center located in two different countries (Antonopoulos and Gillam, 2010). Although the different location data centers belongs to the same cloud provider but each data center in every country are subjected to the laws and regulations of that country and a consumer whose data is important cannot withstand such a risk nor follow up the laws and regulations of other countries (Levandoski, et al., 2013). The situation becomes worst when the data centers hosting a consumer's data is

in a country that is not known for the consumer. This issue should be stated clearly in the service contract and followed up by audits and reviews.

Monitoring by provider: The consumers in general are very proactive in stating confidentiality agreement within the cloud service contracts that preserves the data of the company from being revealed to third parties. In contrast, consumers are less concerned about restricting monitoring activities of service provider itself. Cloud services provider should be prevented by law and contract terms and condition from wide monitoring capabilities to the data. In general, some monitoring tools are required even by the consumer specifically virus and malicious software monitoring and related stuff (Bhardwaj and Kumar, 2011).

Quality of service assurance: A high level of cyber security paradigm level cannot be ensured unless certain level of quality assurance in place and guaranteed. Quality assurance should have certain criteria of quality for each and every category of the service including but not limited to availability, performance and recovery (Kulkarni, et al., 2012; Victor C., et al., 2016).

Service agreement: Service agreements or contracts are the most important framework that defines the cloud service rights and duties of the consumer and the provider. Service agreements define the specifications and arrangements of the service (Youseff, et al., 2008).For companies and institutes that manages their services in-house and do not rely on cloud services providers, internal policies and procedures covers almost the same aspects that are covered and set by the service agreement when cloud services are in use. The following are some of the topics that must be defined in service agreements (Youseff, et al., 2008):

- Terms and Conditions of use and access
- Period of Service
- Renewal and Termination conditions

In some occasions, service agreements are distributed among several agreement documents such as service level agreement, terms of use, and acceptable and privacy policy. The reason for which service agreements are mentioned here as a building block for the proposed secure cloud solution for storage services is that security is highly dependent on the terms defined in the service agreement. There are two important recommendations related to service agreements that should be followed by companies and institutes in order to have a robust secure cloud service:

Non-Negotiated Agreements should not be used:

In predefined service agreements (Palson Kennedy and Gopal, 2010), terms are prescribed by service providers only and are not negotiable. A definite result would be an agreement that is more towards the provider interest and typically lack terms that protects consumer security and privacy. Moreover, in some cases provider have the right to change the terms without the need to consult users and consumers. Such service agreements are very much popular on public cloud services.

Negotiable service agreement is a must for companies and institutes that have security as an important priority. Negotiating the terms in the service agreements paves the way to have full control over security by ensuring that all inherited and introduced cyber security issues are addressed. The following are some points that can improve cyber security and should be negotiated in the service agreement preparation stage (Pedersen, et al., 2011):

- Policy of Security and Privacy
- Procedure of Security and Privacy
- Technical Controls
- Ownership of Data

- Breach notification, and much more

Professional Technical and Legal consultation should be utilized:

The terms of the service agreement highly affects the specifications of the cloud service including the cyber security aspect. In order to have a service agreement that ensures that all current and future cyber security requirements are met, it is important to have a specialized legal and technical teams within the negotiation team force.

Deployment strategy: Specifically for the case of organizational storage requirement, particularly governmental organizations, under consideration private cloud deployment or community is suggested to be utilized. In the assessment (Awad and Abdullah, 2014), one of the organizations was not interested in migrating to cloud services due to his cautiousness about confidentiality. The other organization's network specialist was a little bit easier in that aspect but he may phase difficulties in the management approvals stage due to the same concern. The proposal that is suggested in this paper for governmental organizations or other organizations that are under one umbrella, is to have a community cloud that is managed by government for governmental institutions or managed by a company that belongs to the same corporate for private organizations. Most of the developed countries and a lot of countries in the region have adopted the solution of having a national data center to provide cloud services for critical governmental institution and in that aspect, it is a community cloud deployment method (Singh, et al., 2012).

5.4. Mitigations against introduced cyber security threats of cloud computing

Based on the identified vulnerabilities the following mitigation measures are recommended to be taken.

Shared Multi-Tenant Environment

- High level of assurance of the security mechanisms protecting the logical separation
- Utilizing community or private deployment model of cloud computing

Public Networks exposed services

- Limiting the exposure surface to the minimum possible limit: the priority would be for organizational-owned communication channel. If this option is not possible, then a dedicated channel that belongs to a telecommunication utility is recommended.
- Having an assured minimum bandwidth limit on the communication channel to guarantee the availability required.
- Having a different security and communication scheme for administrative access.

Loss of Control

- For strong legally-backed contract that assures a full compliance by cloud service provider to consumer organization policies and procedures and laws and regulations.
- Continues audit and monitoring of the activities of the cloud service provider.
- Effective reporting mechanism from service provider to consumer that is enforced by the service contract.

In addition, a very essential task to do is the common practices of continuous audits and reviews that are should be supported and agreed in the terms of the service agreement. The above defined threat mitigation strategy is treated as crosscutting security concerns and can be visualize in Figure 1.

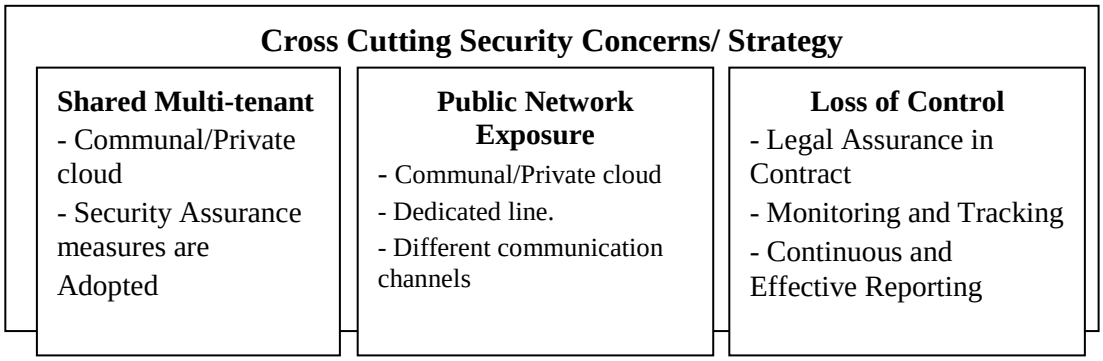

Figure 1 Threat Mitigation Strategy for Securing Cloud Storage

5.5. Proposed Framework

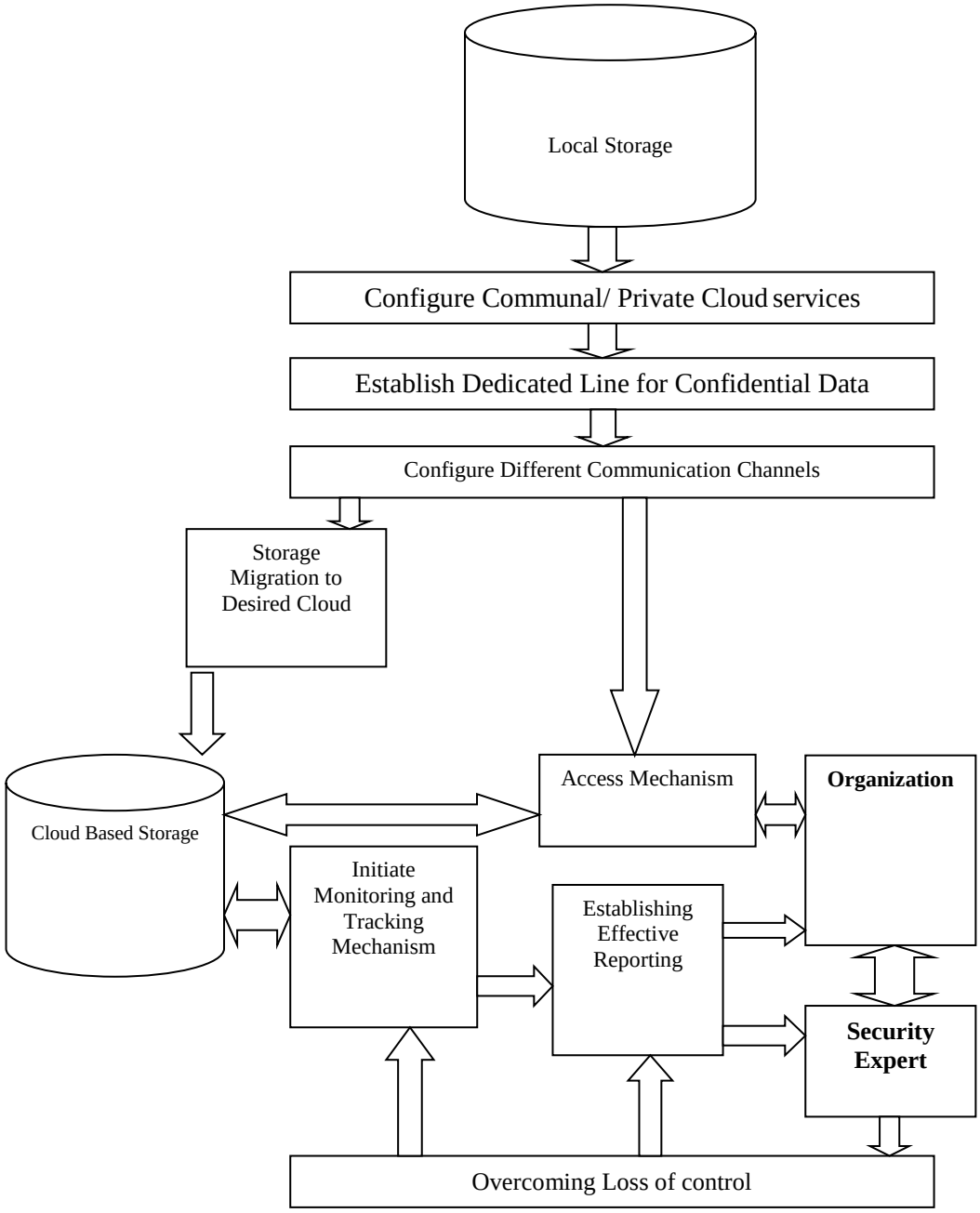

Figure 2 Proposed Framework

Based on the defined crosscutting security concerns for cloud based storage systems in Figure 1, a framework is devised that protects the cloud based storage by overcoming defined vulnerabilities. Figure 2 shows the configuration and operational aspects of proposed framework.

The decision of migration from local storage system to cloud based storage system needs configurations such as communal or private cloud along with the dedicated line access to data. Moreover, it is required to establish clear separation of privileges by defining different communication channels for different users. These configurations ensure the secure storage migration to the cloud with desired security. Once the storage is migrated, it is desired to initiate the monitoring and tracking mechanism to provide trust and control to organization on the relevant cloud services. The organization needs to work hands in hands with specialized security experts to rule out any possible security breaches or concerns. Proposed framework not only highlights the integration of proposed security techniques to secure important storages but also fulfills the objectives set to make use of cloud as baseline storage services to keep scalability intact as well as it secure utilization.

6. CONCLUSION

In the paper, utilization cloud for storage services is assessed. The cyber security aspect of such utilization is thoroughly studied. This study has considered the effect on current security issues in local storage systems and introduces issues due to the nature of cloud computing services. It is found that the utilization of cloud computing for storage systems results in a model that is free of numerous cyber security breaches and vulnerabilities found in the assessment of the Bahraini organizations' local storage systems. It is found also that such utilization introduces new cyber security issues related to the nature of cloud computing. The paper is concluded with a proposed framework for secure utilization of cloud computing for organizational storage requirements. The proposed framework takes into consideration a lot of aspects of cloud services contracts and technological requirements. Deployment model, service model, service contract and mitigations for introduces cyber security issues are all part of the proposal presented. In conclusion, it is found that proper utilization cloud computing for storage services for organizations is the most appropriate approach for organizations nowadays.

7. FUTURE WORK

Current paper elaborates the proposed framework based on the case study conducted for Bahraini organizations. However, the proposed framework can be extended to validate the secure cloud based storage migration for various distributed systems across the globe. This study requires a controlled experiment to be conducted for organization requiring similar configurations and security concerns. Furthermore, this study can contribute to the worldwide researchers' efforts in the relevant field. One possible research track would be of proposing a scientific risk assessment methodology for cloud computing based storage services. The assessment would be of two parts one of which has a questionnaire to be answered by service provider and the other to be answered by service consumer to have the holistic picture clear. Another approach would be interrelated more factors other than cyber security in storage systems local and cloud implementations study.

REFERENCES

[1] Antonopoulos, N., & Gillam, L. (2010). *Cloud computing: principles, systems and applications*, London, Springer Science & Business Media.

[2] Awad, W. S., & Abdullah, H. M., (2014). Improving The Security Of Storage Systems: Bahrain Case Study, *International Journal of Mobile Computing and Multimedia Communications*, 6(3), pp. 78-108.

[3] Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation, *World Congress on Information and Communication Technologies (WICT)*, Iumbai, pp. 217-222.

[4] Bensoussan, K., & SingRu, H.(2011). Impact of security risks on cloud computing adoption, Communication:, *49th Annual Allerton Conference on Control and Computing (Allerton)*, Monticello, pp. 670-674.

[5] Bhardwaj, A., & Kumar, V. (2011). Cloud Security Assessment and Identity Management, *14th International Conference on Computer and Information Technology (ICCIT)*, Dhaka, pp. 387-392.

[6] Bhisikar, P. & Sahu, A. (2013). Security in Data Storage and Transmission in Cloud Computing, *International Journal of Advanced Research in Computer Science and Software Engineering*, 3, pp. 410-415.

[7] Bilski, T. (2007). A Formal Model for Data Storage Security Evaluation, Computational Science and its Applications, ICCSA 2007 International Conference, pp. 253 – 257.

[8] Dawoud, W., Takouna, I., & Meinel, C. (2010). Infrastructure as a service security: Challenges and solutions, *The 7th International Conference on Informatics and Systems (INFOS)*, Cairo, pp. 1-8.

[9] Dinadayalan, P., Jegadeeswari, S. & Gnanambigai, D. (2014). Data Security Issues in Cloud Environment and Solutions, *World Congress on Computing and Communication Technologies (WCCCT)*, Trichirappalli, pp. 88-91.

[10] Gibson, J., Rondeau, R., Eveleigh, D., & Qing Tan. (2012). Benefits and challenges of three cloud computing service models, *Computational Aspects of Social Networks (CASoN), Fourth International Conference on*, pp. 198 – 205.

[11] Hurwitz, J. & Kaufman, M. (2011). *Pravite Cloud for Dummels*, New Jersey, John Wiley & Sons, Inc, Hoboken.

[12] Islam, S.S.,Mollah, M.B., Huq, M.I.& AmanUllah, M. (2012). Cloud computing for future generation of computing technology, *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, IEEE International Conference, pp. 129 – 134.

[13] Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology Gaithersburg, pp. 1-80.

[14] Jiunn-Woei, LianaDavid, C.Yenb & Yen-TingWanga (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital, International Journal of Information Management, 34(1), pp. 28-36.

[15] Koletka, R.& Hutchison, A. (2011). An Architecture for Secure Searchable Cloud Storage, *Information Security South Africa (ISSA)*, Johannesburg, pp. 1-7.

[16] Kulkarni, G., Gambhir, J.,Patil, T., & Dongare, A. (2012). A security aspects in cloud computing, *Software Engineering and Service Science (ICSESS), IEEE 3rd International Conference*, pp. 547 – 550.

[17] Kumar, A., Byung, G. L., HoonJae, L.,& Kumari, A. (2012). Secure storage and access of data in cloud computing, *International Conference on ICT Convergence (ICTC)*, Jeju Island, pp. 336-339.

[18] Leavitt, N. (2009). Is Cloud Computing Really Ready for Prime Time, *IEEE Computer Society*, 42(1), pp. 15-20.

[19] Levandoski, J.J., Larson, P.-A., & Stoica, R. (2013). Identifying hot and cold data in main-memory databases, *Data Engineering (ICDE), IEEE 29th International Conference*, pp. 26 – 37.

[20] Liu, W. (2012). Research on cloud computing security problem and strategy, *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, pp. 1216-1219.

[21] Maddineni, V. & Ragi, S. (2011). *Security Techniques for Protecting Data in Cloud Computing*, Blekinge Institute of Technology.

[22] Mahmood, Z. & Saeed, S., (2013). Software Engineering Frameworks for the Cloud Computing Paradigm.

[23] Mathur, P. & Nishchal, N. (2010). Cloud computing: New challenge to the entire computer industry, *1st International Conference on Parallel Distributed and Grid Computing (PDGC*), Solan, pp. 223-228.

[24] Meetei, M.Z. (2013). Cloud computing and security measure, *Image and Signal Processing (CISP), 6th International Congress*, 2, pp. 852 – 857.

[25] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing, National Institute of Standards and Technology, pp. 1-7.

[26] Mollah, M.B., Islam, K.R., & Islam, S.S. (2012). Next generation of computing through cloud computing technology, *Electrical & Computer Engineering (CCECE) 25th IEEE Canadian Conference*, pp. 1-6.

[27] Muppala, J.K., Hiltunen, M., Robert, S. &Wang, J.(2011). The First International Workshop on Dependability of Clouds, data centers and Virtual Computing Environments, *IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN),*Hong Kong, pp.590-591.

[28] Palson Kennedy, R., & Gopal, T.V. (2010). Assessing the risks and opportunities of Cloud Computing Defining identity management systems and maturity models, *IEEE Trends in Information Sciences & Computing (TISC*), Chennai, pp. 138-142.

[29] Pedersen, J.,M.Riaz, M.T., Celestino Junior, J.,Dubalski, B., Ledzinski, D., & Patel, A. (2011). Assessing Measurements of QoS for Global Cloud Computing Services, Dependable, *Autonomic and Secure Computing (DASC), IEEE Ninth International Conference*, pp. 682 – 689.

[30] Pinto, V. H. S. C., Souza, S. R., & Souza, P. S. (2019, May). A Preliminary Fault Taxonomy for Multi-tenant SaaS systems. *19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pp. 178-187.

[31] Ramachandran, M. (2018). SEF-SCC: Software Engineering Framework for Service and Cloud Computing. In Fog Computing, pp. 227-248, Springer, Cham.

[32] Rao, M. &Sarathy, V. (2009). Cloud Computing and the Lessons from the Past, Enabling Technologies: Infrastructures for Collaborative Enterprises, WETICE '09, 18th IEEE International Workshops, pp. 57 – 62.

[33] Sadiku, M.N.O., Musa, S.M., & Momoh, O.D. (2014). Cloud computing: opportunities and challenges, Potentials IEEE, 33(1), pp. 34-36.

[34] Sharma, K., Kanwar, K., & Yadav, C. (2013). Data Storage Security in Cloud Computing, *International Journal of Computer Science and Management Research*, 2, pp. 1-4.

[35] Singh, R., Kumar, S., & Kumar, S. (2012). Ensuring Data Storage Security in Cloud Computing, *IOSR Journal of Engineering*, 2, pp. 1-5

[36] Suganya, S. & Damodharan, P. (2013). Enhancing security for storage services in cloud computing, *Current Trends in Engineering and Technology (ICCTET), International Conference*, pp. 396 – 398.

[37] VictorC.,Yen H.K.& MuthuR. (2016). Cloud computing adoption framework: A security framework for business clouds, Future Generation Computer Systems, 57, pp 24-41

[38] Wang, C., Wang, Q., Ren, K., & Lou, W. (2009). Ensuring Data Storage Security in Cloud Computing, *17th International Workshop on Quality of Service, IWQoS*, Charleston, pp. 1-9.

[39] Youseff, L., Butrico, M.,& Da Silva, D. (2008). Toward a Unified Ontology of Cloud Computing, *Grid Computing Environments Workshop*, pp. 1 – 10.

[40] Zhou, M., Zhang, R., Wei Xie, Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey, *Sixth International Conference on Semantics Knowledge and Grid (SKG*), Beijing, pp. 105-112.

[41] Charanjeet Singhand Dr. Tripat Deep Singh, (2019) A 3-Level Multifactor Authentication Scheme for Cloud Computing, *International Journal of Computer Engineering and Technology*,10(1), pp. 184-195

[42] Gangu Dharmaraju, J. Divya Lalitha Sri and P. Satya Sruthi, (2016) A Cloud Computing Resolution in Medical Care Institutions for Patient's Data Collection. *International Journal of Computer Engineering and Technology*, 7(6), pp. 83–90

[43] Dr. V. Goutham and M. Tejaswini, (2016) A Denial of Service Strategy to Orchestrate Stealthy Attack Patterns in Cloud Computing, *International Journal of Computer Engineering and Technology*, 7(3), pp. 179–186

[44] Damodar Tiwari, Shailendra Singh and Sanjeev Sharma, (2018) A Prediction Based Multi-Phases Live Migration Approach to Minimize the Number of Transferred Pages, in Cloud Computing Environment, *International Journal of Computer Engineering & Technology*, 9(3), pp. 23–31.

[45] Kuldeep Mishra, Ravi Rai Chaudhary, Dheresh Soni, (2013) A Premeditated Cdm Algorithm in Cloud Computing Environment for FPM, *International Journal of Computer Engineering and Technology*, 4(4), pp. 213–223