Sindh Univ. Res. Jour. (Sci. Ser.) Vol. 47 (3) 463-468 (2015)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Cloud Computing Security Issues: United Arab Emirates (UAE) Perception

S. AHMED, M.N. BROHI[++]

Department of Computer Science SZABIST Dubai, UAE

Received 25th February 2015 and Revised 16th May 2015

Abstract: Cloud Computing is a virtual place of IT organizations that is given to a client over a system on a leased basis and with the capacity to scale up or down their organization fundamentals. Generally, cloud computing organizations are taken by an outside supplier who owns the foundation. Cloud computing gives the client an outsourcing model where the supplier deals with the customer's processing and stockpiling necessities on a pay-as-you-go basis. Organizations need to definitely know the benefits and difficulties particularly for the most basic applications. Security controls in cloud computing are generally the same as security controls in any IT environment. These controls are executed in one or more layers running from the offices (physical security) to the system framework (system security), to the IT framework (framework security) and the distance to the data and applications (application security). Security is noticed as a key requirement when applying cloud computing. This paper presents a detailed examination of the cloud computing security issues perceived by UAE clients including their difficulties concentrating on the cloud computing and the organization transportation types.

Keywords: Cloud Computing, Cloud Computing Security, Cloud Computing Threats, Cloud Computing Models.

1. INTRODUCTION

Cloud computing is a model for enabling an organization customer's persistent, beneficial and on-interest system. Cloud computing gives access to a granted pool of configurable figuring assets (i.e. storage, applications, services network and servers) that could be easily supported and performed with main a administration efforts or administration supplier input, **(**Kangchan 2012).

Cloud computing is another utilization and conveyance model for IT services. The client wanting to use cloud computing does not need any extensive knowledge of a cloud computing system as the requirement of the system is handled by the supplier.
Cloud computing has turned into a real purpose of enthusiasm towards numerous fields with its potential to give improved administration situations alongside the favorable circumstances of adaptability, openness, dependability and superiority while diminishing IT-related working expenses, (Ji-Seong *at el.*, 2013).

Cloud computing has been generally perceived as the cutting edge computing communication, (Hoang *at el.*, 2013).

Cloud computing furnishes the client with an outsourcing del where the supplier deals with the customer's processing and stockpiling necessities on a pay-as-you-go basis, (Jinhui *at el.*, 2010). By joining together a set of present and new procedures from examination regions, for example, virtualization and service-oriented architectures, cloud computing is thusly viewed a computing standard in which assets in the computing organization are given as administrations over the Internet, (Shucheng *at el.*, 2010). It's a well-known fact that cloud computing once applied will reduce the cost, additionally; cloud computing speaks to huge open doors for administration suppliers and ventures. Depending on cloud computing services can manage saving capitals, flexibility and decision making for processing assets.

In spite of the fact that cloud computing can move some control over information and operations from the customer association to its cloud supplier much in the same way, associations endow a piece of their IT operations to outsourcing organizations working a protected cloud-based IT environment. This should be a joined responsibility between the client and the service provider.

Underneath outlined are the two primary situations which we have centered to comprehend the security of the information in the cloud, (Venkata *at el.*, 2011), as shown in **(Fig..1).**

[++]Corresponding Author: M.Nawaz Brohi, +9714366460 mnbrohi@hotmail.com

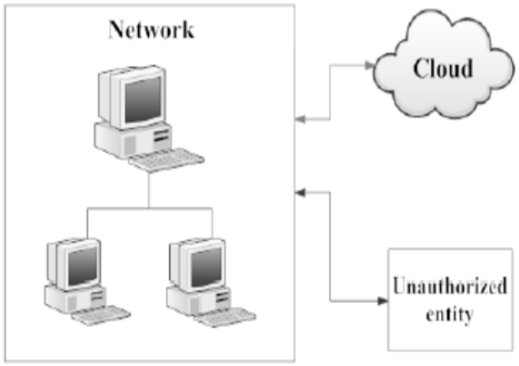


Fig..1 Sensitive Networks (Unauthorized Cloud Computing Access of Data between the Network and Cloud).

This paper is organized as follows: Section 2 will review the related literature along with Cloud Service Models; Section 3 will focus on the related Methods and Material which are used to complete this paper; Section 4 and 5 will explore the ways to collect data to analyze the results and Section 6 and 7 are Conclusion and Recommendations.

2. LITERATURE REVIEW

Cloud computing has a broad scale of services. Public IT based cloud computing, accessible over the web, is changing the way corporate IT administrations are conveyed and administered.

Cloud computing is a web based computing system. It is a set of IT management to facilitate a client on top of a system on a borrowed basis and through the capability to extent up or down their management necessities. The service provider who claims the infrastructure typically will convey cloud computing management, (Kuyoro *el. at.,* 2011). It gives a chance to use shared resources and services from various companies. Although the appearance of cloud computing is growing fast in terms of its concept and in real terms, the economic, the legal, the contractual, the service quality, the inter-networkability, the privacy and the security are still difficulties that need to be dealt with**,** (Jaydip 2013). The security of the cloud computing requisition depends straightforwardly on the cloud computing security. The postulation concentrating on the framework structure of cloud computing, talks about the dangers of the customer security on cloud computing, proposes results on the customer security with its skeleton show and portrays the structure outline, capacity and procedure of the components, (Xu and Yan 2012).

It is fascinating since the cloud could use the appropriate construction modeling of PKI (Public Key Infrastructure) and along these lines build the dependability and cloud computing accessibility and lessening the reaction times for cloud computing acceptance of certificates, (Pankaj *at el.,* 2012). IT procurement is a model of an on-interest administration in cloud computing, frequently focused around dispersed computing innovations and virtualization.

The architectures of cloud Computing have,

- Highly theoretical features vague assets
- Immediate compatibility and adaptability
- Joint Resources (equipment, database, memory, and so on)
- 'Service on demand', typically with a 'pay as you go' charging framework.
- Automatic Administration (e.g., through WS API)

2.1 Services Models of Cloud Computing

Below are the different service models of cloud computing:

a) Software as a service, in this model the requisitions are facilitated and communicated online by means of a web program offering interactively interface usefulness for instance MySAP, Google Docs, and Gmail, (Alvi, *at el.*, 2014)**.**

b) Infrastructure as a service, in this model of cloud computing a set of virtualized assets of computing, for example, computing capability and storage capacity in the cloud are facilitated; consumers can run and organize their personal application stacks to get services, (Alvi, *el. at.,* 2014).

c) Platform as a Service, in this model of cloud computing the cloud gives the product a platform to frameworks (instead of simply programming), the best present illustration being the Google Application Motor, (Alvi, *at el.*, 2014).

3. MATERIAL AND METHODS

In this section we will discuss the selection method which we chose to collect the data to complete this paper, to analyze the data based on the analysis and to generate a result to originate new knowledge.

It includes the selection of data collection methods and data analysis techniques.

The data collection part is done in two phases. The data was collected from the different sources using the following two data collection methods:

- ☐ Online Survey
- ☐ Interviews

In the online survey part we tried to focus on working professionally in the field of IT. Those are

experts in the field of cloud computing and based on their feedback we were able to conclude a good report, which is helpful to produce a clear result.

In the Interview part proper interview questions were written and then conducted. Important key words and ideas were transformed into concepts and then their relationship was found by formulation.

In these both surveys, participates were selected from different organization on the basis of their designation, job description, like CEOs, Presidents, Senior VPs, IT Managers, IT Directors etc. and according to their expertise in the area of cloud computing security like Emirates Airlines, Hospitals, Government Organization, Private companies, working professionals in multinational organizations based in United Arab Emirates (UAE). All are using cloud computing technology in their organizations and based on their feedback we were able to conclude a good report, which is helpful to produce a clear result.

4. DATA COLLECTION

Data was collected according to a predetermined arrangement, which included primary source and direct investigation.

Primary Data: The primary data included several methods mainly interviews, surveys, experiences and observations.

The observation method involved collection of information through analyzing the environment. The one-to-one personal interviews were planned and then conducted in face to face sessions. Online surveys were used randomly where the respondents were sitting in remote locations and the results were collected online. The surveys needed to be designed in a systematic way to ensure its purpose.

5. DATA ANALYSIS

Below is the detailed analysis based on the outcomes of the survey:

5.1 Survey Participants

Below is the chart showing the participants of the survey.

Yes	No	Skipped
40	18	2

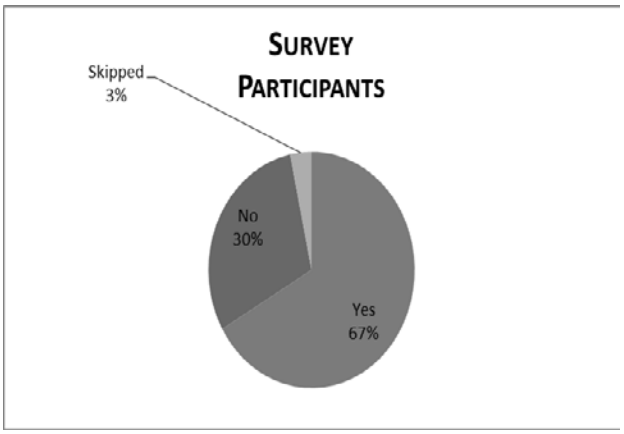


Fig: 5.1 Survey Participants

From the above Fig. **(5.1)** we realize that, the organization is still not completely accepting to adopt the cloud.

5.2 Challenging Factors

Data security is the biggest challenging factor despite of all other challenges stopping organizations to migrate to the cloud. Other challenging factors are also mentioned in Fig. **(5.2)** in detail.

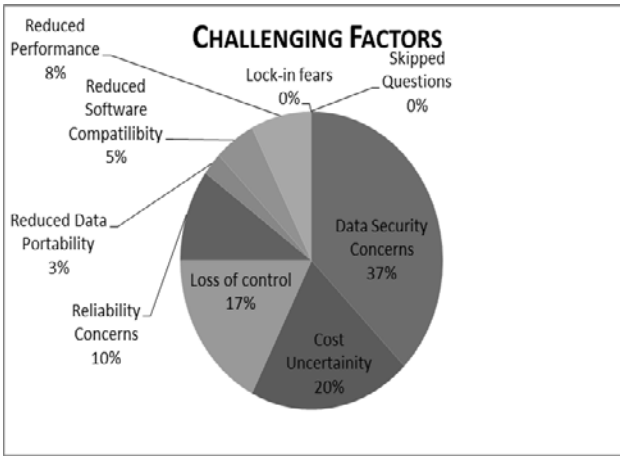


Fig: 5.2 Challenging Factors

5.3 Usage of Cloud Services

Organizations using cloud based services: their main focus is to use the cloud as storage. Despite of all the concerns they are looking to migrate to the cloud. In the below **(Fig.5.3)** we describe other cloud services which are in use.

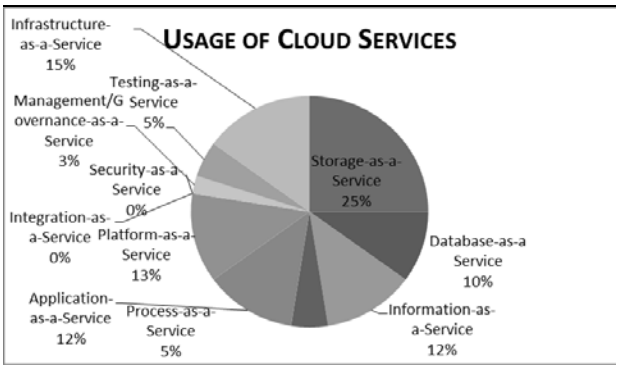


Fig 5.3 Usage of Cloud Computing

5.4 Satisfaction

The Cloud user satisfaction ratio is higher than the dissatisfaction. **(Fig.5.4)** below is showing the detailed results.

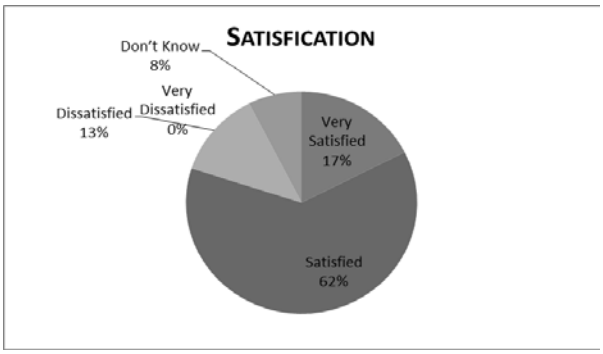


Fig: 5.4 Satisfaction

5.5 Service Issues

Service slow-down is the main reason. Other issues are also there to tackle them. From the service provider point of you service slow-down is the major concern for the cloud user and provider. **(Fig.5.5)** is showing the detailed analysis on Service Issues.

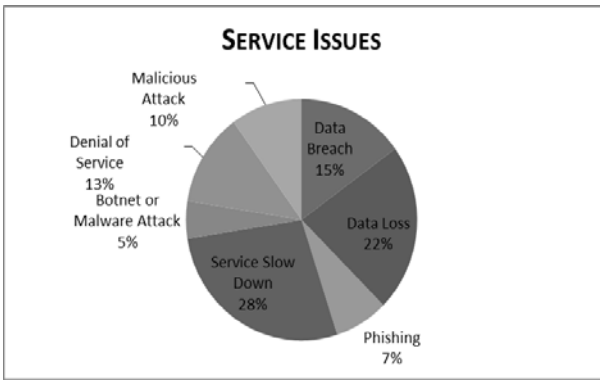


Fig: 5.5 Service Issues

5.6 Total Expenditure

From the enterprise point of view, the expense of the IT department is higher than in comparison to other departments. They are comfortable to migrate to cloud due to the cost cutting point of view despite of any hidden charges even though they have less expense. **(Fig. 5.6)** is showing the detailed results on the Total Expenditure.

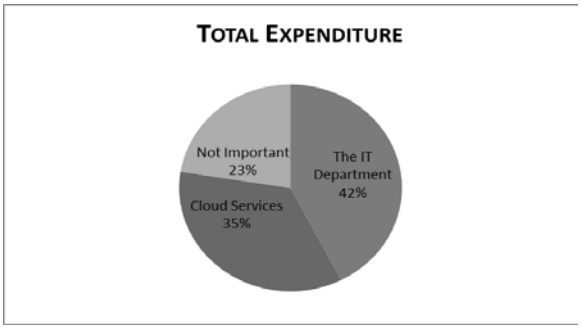


Fig: 5.6 Total Expenditure

5.7 Security Measures

From the security measure point of view the organization's biggest concern is data backup. For details see **(Fig. 5.7).**

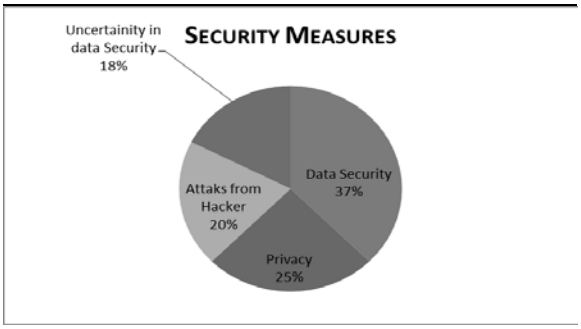


Fig: 5.7 Security Measures

5.8 Security measures to protect business

Companies currently using the following methods, to protect their data from the attacks see **(Fig. 5.8).**

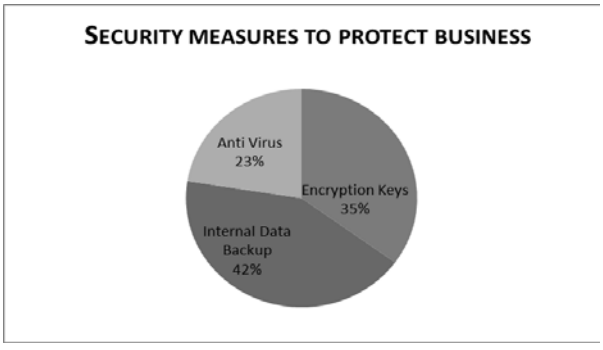


Fig: 5.8 Security Measures to Protect Business

6.

6. CLOUD COMPUTING SECURITY ISSUES IN DIFFERENT COUNTRIES

As cloud computing is becoming more popular and attractive in many countries around the world, across all the continents, it is quite obvious that different countries view cloud computing with different aspects. The most common issues all around the world including UAE, companies need to know whether their data is protected or not and who is responsible for protecting it and whether they are covered financially if the data is exposed. Companies are going into a cloud system too quickly without paying any attention to security. Before migrating to cloud, we have to understand the proper concept of the cloud and how cloud computing should be utilized given unique business requirements. Trust on company's technology, and employees are also major issues for cloud users. We have to protect their environment from data leaks and malicious attacks. Protecting data while transferring and sharing as well as storing requires more attention. In short, security and trust are the main issues in the cloud computing.

Here we are showing a comparison between UAE companies and other companies. The numerous issues mostly worldwide companies including UAE are facing related to cloud security are almost common and given below.

UAE	Other Countries
1. Cloud service issues	1. Access to Servers & Applications
2. Cloud Service	2. Best practices
3. Cloud Storage	3. Cultural issues
4. Cloud user	4. Data Availability
5. Controlling of Data	5. Data Integrity
6. Cost of the service	6. Data Location
7. Cultural issues	7. Data Privacy
8. Data Backup	8. Data Security
9. Data Security	9. Data Segregation
10. Environment	10. Data Transmission
11. Regulatory issues	11. Network Security
12. Total Cost	12. Patch management
13. Total expenditure	13. Regulatory issues
14. Trust	14. Security Policy and
15. Virtual Data Centers	15. Virtual Machine Security

Satisfaction

Satisfaction

Compliance

7. CONCLUSION

The major concern in cloud computing is the security of data, information and the control over it. Despite the fact that respondents are of the opinion that there are a lot of issues in this technology, they still cannot deny the usefulness of its use. According to this study the solution providers are facing challenges in meeting the expectations of their customers and in providing stable cloud services due to the rapidly evolving changes in the technology, but they are still successful in providing the solution with a fair satisfaction level. Cloud computing has given the opportunity to small, medium and Large organizations to use expensive, innovative technology and infrastructure through their creative and capable human resources and professionals for the stabilization of the Cloud computing business domain. Those users who are not directly using the cloud computing services are concerned about the security issues, total cost of the service and the environment, while the direct and primary user mainly focuses on the cost. This gives the idea that users of the technology provide the main parameters of quality and satisfaction of the services level in the industry and the solution providers can design their solutions according to that. The need for further innovation and advancement is required so that the solutions are more cutting edges and are economical in order to reach everyone.

8. RECOMMENDATIONS

The service providers should follow one of the data standards model like SOX, PCI DSS or ISO and report the compliance status to the partner organizations to build a trustworthy relationship. Both Security and Trust are the main issues between the service provider and the client while migrating to the cloud from the local premises. Both the service provider and the client have to push, specially the client, to start to use the cloud services by migrating their lower staff data (outlook) to the cloud to build trust and step by step migrate to the cloud from the lower to the top management. Dedicating a lot of resources and services to audit the data like enterprise security and taking a lot of time to secure their data on the cloud like as enterprise organization, they are using a cloud network with a lot of hidden layers and tolls in the cloud work like your own domain. Clients should choose the data destination path (server location) as per their data sensitivity. In this research, big organizations normally prefer to migrate the data to Swiss. As the main concern of every organization is security and trust, following are the findings of this research:

- One Server as a backup in the premises of the organization due to the following reason
  - Data lost
  - Compromise Security
  - Internet Connectivity Problem

At last the authentication method should be two to three layers (i.e. User id, p/w, Public Key, Private Key).

The benefits of the above recommendations are to avoid all the concerns without any interruption in services.

REFERENCES:

Alvi, F. A. (2014). Review on cloud computing security issues & challenges, (white paper) - Department of Computer Systems and Electronic Engineering, QUEST Nawabshah, Sindh, Pakistan.

Hoang T. D., C. Lee, D. Niyato, and P. Wang.(2013). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless Communication and Mobile Computing, 13(18):1587–1611.

Jaydip S. (2013). Security and Privacy Issues in Cloud Computing. Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.

Ji-Seong J., M. Kim, and Kwan-HeeYoo (2013). A Content Oriented Smart Education System based on Cloud Computing. International Journal of Multimedia and Ubiquitous Engineering 8(6):313-328.

Jinhui Y., (2010). Accountability as a Service for the Cloud. IEEE International Conference on Services Computing, Miami, FL: 81-88.

Kangchan L. (2012). Security Threats in Cloud Computing Environment. International Journal of Security and Its Applications, 6(4):25-32.

Kuyoro S. O., F. Ibikunle O. Awodele (2011). Cloud Computing Security Issues & Challenges, International Journal of Computer Networks *(*IJCN), 3(5):247-255.

Pankaj A., and R. C. Wadhawan (2012). Enhancing Security and Privacy In The Cloud, International Journal of Computing and Corporate Research, 2(2).

Shucheng Y., (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. Proceedings IEEE, San Diego, CA 2010: 1-9

Venkata S., K. Maddineni S. Ragi (2011). Security Techniques for Protecting Data in Cloud Computing, Master Thesis Electrical Engineering. School of Computing. Blekinge Institute of Technology SE - 371 79 Karlskrona Sweden.

Xu X., and Y. Junhub (2012). Research on Security of the Client Based on Cloud Computing. 2012 International Conference on Artificial Intelligence and Soft Computing Lecture Notes in Information Technology, Vol. 12. 1-6