International Journal of Computer Applications in Engineering Sciences
[VOL II, ISSUE III, SEPTEMBER 2012] [ISSN: 2231-4946]

ISM for Analyzing the Interrelationship between the Inhibitors of Cloud Computing

Ambika Devi Amma.T[1], Pramod V. R [2], Radhika. N[3]

[1]*Research scholar, Karpagam University. Coimbatore, Tamil Nadu*
[1]*Dept .of Computer Science and Engineering, NSS College of Engineering, Palakkad, Kerala, India 678008*
[2]*Dept. of Mechanical Engineering, NSS College of Engineering, Palakkad, Kerala, India 678008*
[3]*Computer Science and Engg Dept, Amrutha University, Coimbatore, Tamil Nadu, India 641105*

[1]prof.ambikadevit@gmail.com
[2]pramodram09@gmail.com
[3]n_radhika@cb.amrita.edu

***Abstract*— Interpretive structural model (ISM) is well proven for establishing the interrelationship between the variables influencing the system. The strategy of clouding is subjected to many inhibitors. This paper deals with the deployment of ISM to model the interrelationships between the inhibitors of cloud computing. The model is made which is based on SSIM, initial reachability matrix, final reachability matrix and diagraph. Finally the Inhibitors are classified into four clusters based on their driving power and dependence. In this way action plan has been formulated for mitigating the most sensitive inhibitors.**

***Keywords*— ISM, Clouding, Driving power-dependence diagram, Diagraph.**

I. INTRODUCTION

Cloud Computing is a new scenario in which customers can use the services and infrastructures by paying an amount for the usage. This is beneficial to some of the IT organizations undergoing severe budgetary constraints for the development of infrastructures and enhancement of hardwares and softwares. The core technologies used in cloud are web applications, services, virtualization and cryptography. The services rendered through cloud are Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). In Software as a Service, the service providers provide the users the service of using any type of application software. In IaaS, the service providers provide the networking equipment, storage backups and servers. In PaaS the service providers provides the platform to the users any type of operating systems along with hardwares & Softwares.

The deployment models available for cloud are private cloud, public cloud and hybrid cloud. In public cloud the users are accessing the cloud services using internet facilities. Private cloud provides resources to users within an enterprise or organization over an intranet using a self service interface. Hybrid cloud is a combination of both public cloud and private cloud. In hybrid, the private clouds can break through the private cloud to access additional computing resources from the public cloud.

The main characteristics of clouds are (a) On demand self service- Users can use the services without human interaction (b) Ubiquitous network access- Using standard mechanisms and protocol cloud services are accessed using network usually internet. (c) Resource pooling:- Resource pooling is done using a homogeneous sharing between service users. (d) Elasticity: Resources can be stored up and down rapidly. (e) Pay-as-you-go: Resource usage is constantly measured and pay only for what you use.

Some of the IT organizations are undergoing severe budgetary constraints depends on clouds for the infrastructure and services. The strategy of cloud computing is facing many barriers. The major attributes of cloud computing are multitenency, massive scalability, elasticity, pay as you use and self provisioning of resources of the cloud[1]. An acronym "SPI" stands for the services of the cloud, Software–as-a-Service (SaaS), Platform-as-a-Servive (PaaS) and Infrastructure-as-a-Service (IaaS) [1]. Cloud computing impacts an individual consumer, individual business, small and medium size businesses and enterprise businesses etc. Data are moving from and into the cloud in large amounts, so the security control failures or impact of mistakes will affect the customers. The idea behind the paper is to get the inhibitors in the cloud environment and make a study under ISM and get the relationship among the inhibitors. The aim of this paper is to develop relationship among the major inhibitors of cloud computing using interpretive structural modeling (ISM) and classifying this inhibitors depending upon their driving power and dependence power. ISM is a methodology for identifying relationship among specific items [9,10,11]. Inhibitors

as the name indicates always acts as barriers for the full fledged implementation of any new methodology. Inorder to reap the full benefits of the new methodology and to prove good return on investment, those inhibitors have to be suppressed appropriately. At the outset, inhibitors have been extracted from literature source. They were further confirmed by experts from industries and academia. In this way 18 inhibitors were identified which are depicted in table 1.

Inorder to increase the readability of the article, a brief enumeration of the term is given below.

- Lack of sufficient security: is related to the security concern of the cloud services. Security should include browser security also.
- Lack of reliability: The customer should feel that the services done by the cloud service provider is reliable in the sense the data's attaining from the cloud is correct. It is not assured.
- Lack of portability: The data stored in one country can be transferred to another data centre in another country. A pointed violation of local law may result.
- Lack of privacy: It is the accountability to data &transparency to organizations personal informations.
- Lack of standardization: Standards are source within the cloud mass adoption.
- Lack of comprehensive tool management: These tools would help automatic server providing and aids with capacity planning and configuration management.
- Week access control: The ability to manage the infrastructure is weak more control to manage servers, networking and cabling are weak.
- Lack of data confidentiality: Authorization and authentication relate to confidentiality. Confidentiality depends on how data put into the cloud will be secure and available
- Ineffective backup management: Lack of how effective backup of data.
- Cost/time management: Cost/time barrier should be evaluated closely as a cloud migration.
- Network Management: Cloud services are done through internet world wide web. Managing the network is a tedious process.
- Legal issues: Cloud data migration from one country to another face legal issues.
- Infrastructure Security:- In network level – Network topology should be changed according to the security requirement.
- Infrastructure Security: In host level, depends on the delivery models like SaaS, PaaS, IaaS and deployment models like private, public and hybrid.
- Infrastructure Security: In application level- depends on the revolution of current practices and security in application.
- Data Security: Data should be protected without making any processing on it.

Data Integrity: What a customer wants to do is to validate the integrity of data while that data remains in the cloud.

Data availability: Data should be available for the customer at their needs, highly available database form is more complex.

TABLE 1: MAJOR INHIBITORS OF CLOUD COMPUTING

Inhibitors Number	Major Inhibitors of Cloud Computing	References
1	Lack of sufficient security	[1], [2], [4], [6],
2	Lack of reliability	[1], [2], [4], [6],
3	Lack of portability	[1], [2],[18]
4	Lack of privacy	[1], [2],[18]
5	Lack of standardization	[1], [2],[18]
6	Lack of comprehensive	[1], [2],[18]
7	Weak access control	[1], [2],[18]
8	Lack of data confidentiality	[1], [2],[18], [31]
9	Ineffective back up	[1], [2],[18]
10	Cost/ time barrier	[1], [2],[18]
11	Network management barrier	[1], [2],[18]
12	Legal issues	[1], [2],[18],[31]
13	Infrastructure security –at	[1], [2],[18]
14	Infrastructure security –at host	[1], [2],[18]
15	Infrastructure security –	[1], [2],[18]
16	Data security	[1], [2],[18],[31]
17	Data integrity	[1], [2],[18],[31]
18	Data availability	[1], [2],[18]

II. LITERATURE SURVEY

The inhibitors of cloud computing have been identified from various authors who have researched and written directly in their issues. The security issues of cloud computing [1,2,3] privacy is the most important security issue. Privacy obligations are related to how the cloud service control is hosted in the company. Clouds can close multiple jurisdictions [1,8,9]. The privacy law in different country may be different [1].

Cloud computing is a large scale distributed computing paradigm that is driven by economies of scale in which a pool of abstracted virtualized, dynamically scalable , managed computing power, storage, platforms and service are delivered on demand to external customers over the internet. Technologically, cloud computing indeed evolved out grid computing, utility computing and virtualized technology. Computing resources are provided as a public utility,

and can be used anytime anywhere. Cloud manufacturing is a service oriented networked manufacturing paradigm supported by cloud computing. Utility computing and Service Oriented Architecture (SOA) which provides manufacturing services on demand according to the requirement of end user through internet. It completely overturns the production-oriented manufacturing to service oriented. Companies may rent/buy time slots to perform manufacturing task on demand through this platform [Quan Liu, Lu Gao, Ping Lou,2011]

In cloud computing technology there are a set of important policy issues, which include issues of privacy security, anonymity, government surveliance, reliability and liability among others. But most important between them is security and new cloud provider assures it.

All users who use same virtual machine as infrastructure, if a hacker steals a virtual machine and take control over it, he will be able to access all users data within it. The hacker can copy them in to his local machine before cloud provider detect that virtual machine is out of control [Farzad Sabahi, 2011]. Cloud computing depends on the internet technology hence it faces the same risks of internet. Distributed denial of service is one of the most powerful attack facing by cloud. The main issues of cloud computing are data location and data segregation. Because of this many enterprises are hesitating to use the cloud service for their sensitive datas. Only less sensitive datas are migrated to the cloud [Farzad Sabahi-2011]. Data access and interoperability are the major issues affecting cloud computing [Craig A Lee] cloud computing can provide very rapid growth to the economy of rural areas by providing information technology for efficient business management. To realize the full protential of cloud computing and to be mainstream member of IT portfolio and choices, the challenges has to be met. There is a lot of challenges to be tackled related to privacy and security and associated regulations compliance vendor lock-in and standards, interoperability, latency, performance and reliability concern besides. R &D and treating specific testbeds in public private partnership. Cloud computing has wide filed of applications in the current scenario. Recently it has powered its foot prints in networking web and software services (Sasikala 2011). The popularity of cloud offerings one primarily one the financial benefits gained by the organization when comparing to a premise investments. The cloud infrastructure consists of large number of parallel servers operating in distributed networking environment mainly using virtualization technology. Many application programming interfaces are used for developing user friendly programs to run in software as a service mode [Peiris.C, Sharma .D-2011].

Cloud computing collects the computing resources and manages them automatically through software virtualization improves service capacity. The users can compare and select service providers. Example of clouds are Google owned more than one million servers. Amazon, IBM Microsoft, Yahoo they have thousands of servers. In cloud computing the user or applications can directly send to management node from there to the concerned servers. Effectively all the CPU resources are shared and distributed as if a single server environment. Cloud computing evolution may be affected by the regulatory lows and orders cloud computing services paradigms creates a set of major security and privacy risks . These issues can harm the cloud service computing [Reijo M Savola 2010 IEEE]. For the past 25 year ISM has been issued as an effective methodology for dealing with complex issues. Interpretive structural modeling (ISM) is a computer assisted learning process [J. Warfiled 1973]

III. METHODOLOGY

ISM methodology has been used to impose order and direction on the complexity of relationships among elements of a system. It is the interpretive of the group decides, how the variables are related. It is structural since the overall structure is extracted on the basis of relationship among the set of variables. In this technique, the specific relationships and overall structure are portrayed in a graphical model.

The steps involved in this techniques are

- The elements are identified.
- A relationship between elements are established with respect to the elements to be examined.
- Develop a structural self interaction matrix (SSIM)
- From SSIM a reachability matrix is constructed from reachebility matrix driving power and dependencies are calculated.
- Level partition of elements are done considering reachability set antecedent set and intersection.
- A diagraph is constructed based on the level partition.
- ISM model is constructed from the diagraph.

Graph is constructed with dependence and driving power. From the graph elements are classified as autonomous, dependent, linkage and independent.

A. Structural Self Interaction Matrix (SSIM)

After consulting with group experts from different industries the nature of contextual relationship among the barriers were identified. [See Table1]. For analyzing the barriers in constructing SSIM, the following four symbols have been used to denote the direction of relationship between barriers (i and j)

V- variable i will help to achieve variable j

A- variable j will help to achieve variable i
X-variables i and j will help each other
O-variables i and j are unrelated

TABLE 2- STRUCTURAL SELF INTERACTION MATRIX (SSIM)

		18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2
1	Lack of sufficient	V	V	V	A	V	V	0	V	0	A	V	V	0	0	A	0	V
2	Lack of reliability	V	V	V	A	A	A	V	V	0	A	V	0	A	V	0	0	
3	Lack of portability	V	V	0	0	0	0	V	V	A	0	0	0	0	A	0		
4	Lack of Privacy	V	V	V	0	0	0	V	0	0	0	A	V	0	0			
5	Lack of Standardization	X	V	A	A	A	A	V	V	A	0	V	A	X				
6	Lack of comprehensive management tool	0	0	0	A	A	A	0	A	A	0	0	A					
7	Weak access control	V	V	V	V	V	V	0	0	0	0	A						
8	Lack of data confidentiality	V	V	V	V	V	V	0	A	0	0							
9	In effective backup management	V	V	V	V	0	0	0	0	0								
10	Cost/time barrier	V	V	V	V	0	0	V	0									
11	Network management barrier	0	0	0	0	V	V	V										
12	Legal issues	V	V	0	0	0	0											
13	Infrastructure security network level	V	V	V	V	V												
14	Infrastructure security – host level	V	V	V	A													
15	Infrastructure security –application level	V	V	V														
16	Data security	V	V															
17	Data Integrity	V																
18	Data availability																	

B. Reachability Matrix

SSIM has been converted into a binary matrix, called initial reachability matrix by substituting V,A,X and O by 1 and 0 as per the given case. The substitution of $1'^{S}$ and O'^{S} are as per the following rules.

- If the (i,j) entry in thr SSIM is V, the (i,j) entry in the reachability matrix becomes 1 and the (j,i) entry becomes 0;
- If the (i,j) entry in the SSIM is A, the (i,j) entry in the reachability matrix becomes O and the (j,i) entry becomes 1;
- If the (i,j) entry in the SSIM is X, the (i,j) entry in the reachability matrix becomes 1 and the (j,i) entry also becomes 1; and
- If the (i,j) entry in the SSIM is O, the (i,j) entry in the reachability matrix becomes 0 and the (j,i) entry also becomes 0.

Initial reachability matrix thus constructed is as shown in table 3. There is no transitivity in this case initial reachability matrix will be used for further calculations. The driving power and dependence are shown in Table 4.The driving power for each element is the total number of elements (including itself) which of may help achieve. Dependence is the total number of elements which may help achieve it.

C. Level Partitions

From the financial reachability matrix , the reachability and antecedent set for each element is found[37]. The reachability set consists of the elements and other elements which may help to achieve it. The antecedent set consist of the element and other elements which may help in achieving it. After getting reachability set and antecedent set intersection set is derived for all elements. The element for which the reachability and the intersection sets are the same occupy the top level in the ISM hierarchy. The top level element would not help achieve any other element above its own level, The top-level element is separated from other elements. The same process is repeated to find out the next level elements. This process is continued until the level of each element is found. These levels are used for building diagraph and the final model.

TABLE 3: INITIAL REACHABILITY MATRIX

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	1	0	0	0	0	1	1	0	0	1	0	1	1	0	1	1	1
2	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	1	1
3	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1
4	1	0	0	1	0	0	1	0	0	0	0	1	0	0	0	1	1	1
5	0	0	1	0	1	1	0	1	0	0	1	1	0	0	0	0	1	1
6	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	1	1	1	0	0	0	0	0	1	1	1	1	1	1
8	0	0	0	1	1	0	1	1	0	0	0	0	1	1	1	1	1	1
9	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	1	1
10	0	0	1	0	1	1	0	0	0	1	0	1	0	0	1	1	1	1
11	0	0	0	0	0	1	0	1	0	0	1	1	1	1	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1
13	0	1	0	0	1	0	1	1	0	0	0	0	1	1	1	1	1	1
14	0	1	0	0	1	0	1	1	0	0	0	0	0	1	0	1	1	1
15	1	1	0	0	1	0	1	1	0	1	0	0	0	0	1	1	1	1
16	0	0	0	1	1	0	1	1	0	1	0	0	0	0	0	0	1	1
17	0	0	0	1	0	0	1	1	0	1	0	0	0	0	0	0	1	1
18	0	0	0	1	1	0	1	1	0	1	0	0	0	0	0	0	0	1

TABLE 4: FINAL REACHABILITY MATRIX WITH DRIVING POWER AND DEPENDENCE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	DP
1	1	1	0	0	0	0	1	1	0	0	1	0	1	1	0	1	1	1	10
2	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	1	1	8
3	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	5
4	1	1	0	1	0	0	1	1	0	0	1	1	1	1	0	1	1	1	12
5	0	0	1	0	1	1	0	1	0	0	1	1	0	0	0	0	1	1	8
6	0	1	0	0	1	1	0	1	0	0	1	1	0	0	0	1	1	1	9
7	0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	14
8	1	0	0	1	1	0	1	1	0	0	0	1	1	1	1	1	1	1	12
9	1	1	0	0	0	0	1	1	1	0	1	0	1	1	1	1	1	1	12
10	0	0	1	0	1	1	0	0	0	1	1	1	0	0	1	1	1	1	10
11	0	1	0	0	1	1	0	1	0	0	1	1	1	1	0	0	0	0	8
12	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	3
13	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	1	1	1	12
14	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	1	1	1	10
15	1	1	0	0	1	0	1	1	0	1	1	0	1	1	1	1	1	1	13
16	1	0	0	1	1	0	1	1	0	1	0	1	0	0	0	1	1	1	10
17	1	0	0	1	0	0	1	1	0	1	0	1	0	0	0	1	1	1	9
18	1	0	0	1	1	0	1	1	0	1	0	1	0	0	0	1	1	1	10
DEP	8	9	4	6	12	5	11	15	1	5	13	15	8	9	6	14	17	17	

TABLE 5 LEVEL PARTITION OF ELEMENTS - 1ST LEVEL

Elements	Reachability Set	Antecedent Set	Intersection	Level
1	1,2,7,8,11,13,14,16,17,18	1,4,8,9,15,16,17,18	1,8,16,17,18	
2	2,5,8,11,12,16,17,18	2,4,6,9,11,13,14,15	2,11	
3	3,11,12,17,18	3,5,7,10,11	3,11	
4	1,2,4,7,8,11,12,13,14,16,17,18	4,7,8,16,17,18	4,7,8,16,17,18	
5	3,5,6,8,11,12,17,18	2,5,6,7,8,10,11,13,14,15,16,18	5,6,8,11,18	
6	2,5,6,8,11,12,16,17,18	5,6,7,10,11	5,6,11	
7	3,4,5,6,7,8,11,12,13,14,15,16,17,18	1,4,7,8,9,13,14,15,16,17,18	4,7,8,13,14,15,16,17,18	
8	1,4,5,7,8,12,13,14,15,16,17,18	1,2,4,5,6,7,8,9,11,13,14,15,16,17,18	1,4,5,7,8,13,14,15,16,17,18	
9	1,2,7,8,9,11,13,14,15,16,17,18	9	9	
10	3,5,6,10,11,12,15,16,17,18	10,15,16,17,18	10,15,16,17,18	
11	2,5,6,8,11,12,13,14	1,2,3,4,5,6,7,9,10,11,13,14,15	2,5,6,11,13,14	
12	12,17,18	2,3,4,5,6,7,8,10,11,12,13,14,16,17,18	12,17,18	1
13	2,5,7,8,11,12,13,14,15,16,17,18	1,4,7,8,9,11,13,15	7,8,11,13,15	
14	2,5,7,8,11,12,14,16,17,18	1,4,7,8,9,11,13,14,15	7,8,11,14	
15	1,2,5,7,8,10,11,13,14,15,16,17,18	7,8,9,10,13,15	7,8,10,13,15	
16	1,4,5,7,8,10,12,16,17,18	1,2,4,6,7,8,9,10,13,14,15,16,17,18	1,4,7,8,10,16,17,18	
17	1,4,7,8,10,12,16,17,18	1,2,3,4,5,6,7,8,9,10,12,13,14,15,16,17,18	1,4,7,8,10,12,16,17,18	
18	1,4,5,7,8,10,12,16,17,18	1,2,3,4,5,6,7,8,9,10,12,13,14,15,16,17,18	1,4,5,7,8,10,12,16,17,18	

IV. ANALYSIS USING ISM

All the element have been classified based on their driving power and dependence power into four categories. They are 1. Autonomous 2. Dependent 3. Linkage 4. Independent. It is observed that element 3 has a driving power of 5 and dependent power of 4. As hown in figure-1The objective behind the classification is to analyze the driving power and dependent power of the elements. In this classification the first cluster is autonomous, having low dependence and low driving power. The autonomous elements are weak, here element 3 is autonomous. The second cluster is having low driving power and high dependence power. Here element 12 is in this category. The third cluster consists of linkage barriers having high driving power and high dependence power. Any action on this elements will have an effect on other elements. Here elements 2,5,7,8,11,14,16,17 and 18 are under linkage category. The fourth cluster is independent having high driving power and low dependence power . The elements 1,4,6,9,10,13,15, are under independent category.

TABLE 6 OTHER LEVELS

Element	Reachability	Antecedent	Intersection	Level
1	1	1,4,9	1	8
2	2,16	1,2,4,9,13,14,15,16	2,16	4
3	3,11	3,5,7,10,11	3,11	2
4	4	4	4	9
5	5,6,8	2,5,6,7,8,10,13,14,15,16	5,6,8	3
6	5,6,8	2,5,6,7,8,10,13,14,15,16	5,6,8	3
7	7,14	1,4,7,13,14,15	7,14	5
8	5,6,8	2,5,6,7,8,10,13,14,15,16	5,6,8	3
9	9	9	9	9
10	10,15	10,15	10,15	6
11	3,11	3,5,7,10,11	3,11	2
12	12,17,18	2,3,4,5,6,7,8,10,11,12,13,14,16,17,18	12,17,18	1
13	13	1,4,9,13	13	7
14	7,14	1,4,7,13,14,15	7,14	5
15	10,15	10,15	10,15	6
16	2,16	12,4,9,13,14,15	2,16	4
17	12,17,18	12,4,9,13,14,15	12,17,18	1
18	12,17,18	12,4,9,13,14,15	12,17,18	1

V. DEVELOPMENT OF ISM DIAGRAPH AND MODEL

From the initial reachability matrix (see table-) the structural model is generated. If there is a relationship between the elements i and j an arrow points from i to j is used for presentation. This graph is known as diagraph. The diagraph is converted into the ISM based model.

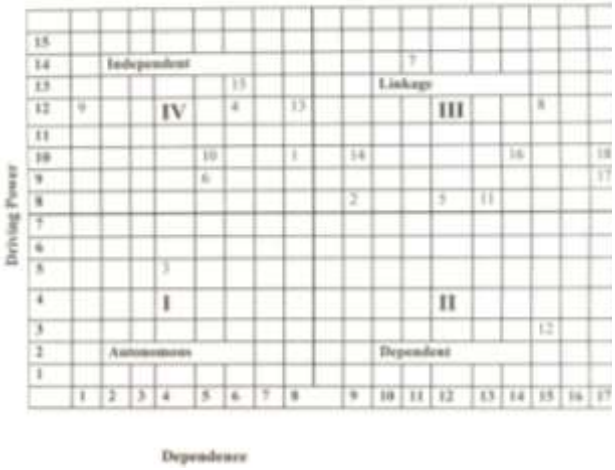

Fig. 1 Driving Power dependence Diagram

VI. 6. RESULTS AND DISCUSSIONS

The levels of the elements are important. Privacy and ineffective back up management are the most important due to its high driving power and low dependence among all the elements. This can be validated by the previous survey results[1,]. This element is positioned at the lowest level in the ISM based model. Legal issues at the highest level in the ISM model due to its high dependence power and low driving power.

The driving power and dependence power give some valuable insight about the importance and independence of the elements. The driving power

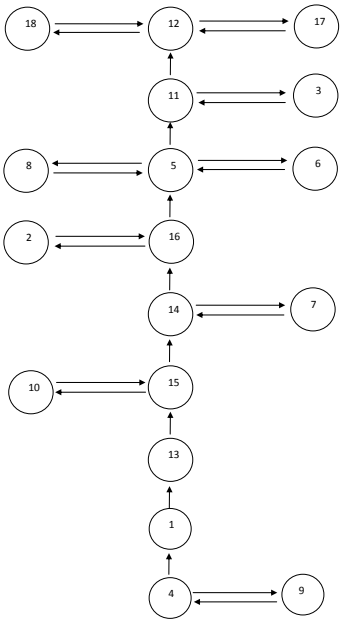

Fig. 2 ISM Diagraph

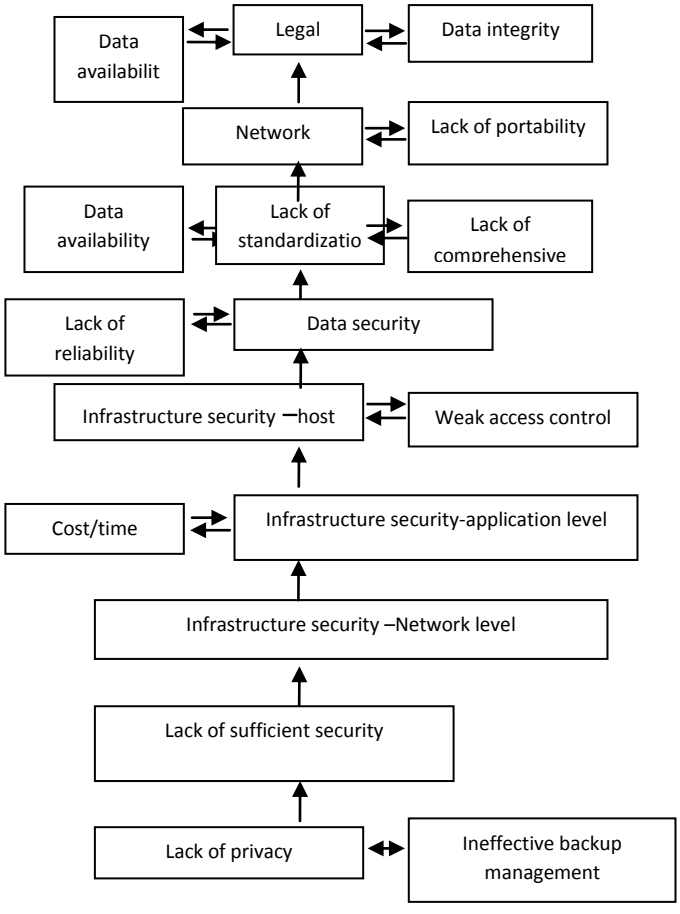

Fig. 3 Interpretive Structural Model

and dependence power diagram indicates only one element in autonomous region. Autonomous elements have low dependence power and low driving power . These elements have not much influence in the system. Linkage element 2,5,7,8,1,14,16,17&18 are lack of reliability, lack of standardization , weak and access control, lack of data confidentiality network management barrier, infrastructure security-host level, Data security, Data integrity and data availability respectively. Independence section have high driving power and low dependence power. The elements are 1,4,6,9,10,13,15. They are lack of sufficient security, lack of privacy, lack of comprehensive management, in effective back up management, cost/time barrier infrastructure security network level, infrastructure security-applications levels.

VII. Conclusion And Future Scope

Result analysis shows that some of the elements have weak driving power and dependency which can be disconnected from the structure. The elements having strong driving power and dependencies affect the system. The study pinpoints the importance of various elements to the structural flexibility. T security concern is very critical to cloud computing. The levels of elements are very important for modeling the inhibitors for loud computing. Lack of sufficient security, lack of privacy, lack of comprehensive management tool ineffective backup management, cost/time barrier, infrastructure security-application level have high driving power and less dependence power. Therefore these elements are the key elements for cloud computing. All the fifteen elements considered are very important. As a future scope the fuzziness among the interrelationship can be tested by fuzzy ISM. In addition to that the validation of threshold can be ascertained by ISM model. The experts were busy with the job schedules. They had some limitations to provide much time for research. This is a limitation for the study even though the familiarity of the respondents has been explored to compensate it to a significant extent.

Cloud technology is paid for what we use. Thereby saving the conomy of the organization. Organization can store bulk of data then storing in their private computer system. The software is highly automated no need for keeping it up to date. The flexibility is increased. Customer can access information wherever they are. Customers are free from the updation of server and other computing resources.

The importance of the structural flexibility of the inhibitors are derived from the graph relating driving power and dependency. Inhibitors are the variables which well influence the system. An interrelationship among the inhibitors can be established using ISM. In ISM diagraph the vertices represent the elements of the issue or the problem being studied.

The elements are classified depending upon the driving power and dependence relation. If the driver power and dependence are low then that inhibitors are not strongly related to the system. That inhibitors can be even disconnected from the system. Result indicates that out of eighteen inhibitors only one inhibitor is having low driving power. This elements are known as autonomous.

References

[1] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy- AnEnterprise Perspective on Risks and Compliance" O Reilly

[2] Wang.C and Wulf W. A., "Towards a framework for security measurement", 20th National Information Systems Security Conference, Baltimore, MD, Oct. 1997, pp. 522-533.

[3] Savola.R and Abie.H, "Development of measurable security for a distributed messaging system," International Journal on Advances in Security, Vol. 2, No. 4 (2009), 2010.

[4] Jaquith. A, "Security metrics: replacing fear, uncertainty and doubt,"Addison-Wesley, 2007.

[5] Gadia.S, "Cloud computing: an auditor's perspective," ISACA Journal, Vol. 6, 2009.

[6] Gellman.R, "Privacy in the clouds: risks to privacy and confidentiality from cloud computing," World Privacy Forum (WPF) Report, Feb. 23, 2009.

[7] Cloud Security Alliance, "Top threats to cloud computing", Version 1.0. Downloaded from: www.cloudsecurityalliance.org [July 4, 2010].

[8] Cloud Security Alliance. www.cloudsecurityalliance.org [July 4, 2010].

[9] Mandal.A, Deshmukh.S, Vendor selection using interpretive structural modeling (ism). International Journal of Operations and Production Management, 1994, 14(6): 52–59.

[10] Sage.A, Interpretive Structural Modeling: Methodology for Large-scale Systems, 91–164. McGraw-Hill, New York, 1977.

[11] Warfield.J. Developing interconnection matrices in structural modeling. IEEE Transactionsons on Systems, Man and Cybernetics, 2005, 4(1): 81–67.

[12] Wang.C, "Forrester: A close look at cloud computing security issues," http://www.forrester.com/ securityforum 2009, 2009.

[13] IDC, "It cloud services user survey, pt.2: Top benefits & challenges," http://blogs.idc.com/ie/?p=210, 2008.

[14] Zetta, "Zetta: Enterprise cloud storage on demand," http://www.zetta.net/, 2008.

[15] Chen.P, Lee.E, Gibson.G, Katz.R, and Patterson.D, "RAID: High performance,reliable secondary storage," ACM Computing Surveys (CSUR), vol. 26, no. 2,pp. 145–185, 1994.

[16] Yahoo!, "Hadoop distribted file system architecture," http://hadoop.apache.org/common/docs/current/hdfs design.html, 2008.

[17] Dwork.C et al., "Differential privacy," LECTURE NOTES IN COMPUTER SCIENCE, vol. 4052, p. 1, 2006.

[18] Dwork.C, "Differential privacy: A survey of results," Lecture Notes in Computer Science, vol. 4978, p. 1, 2008.

[19] Dean. J and Ghemawat.S, "MapReduce: simplified data processing on large clusters," in Proceedings of the 6th conference on Symposium on Opearting Systems Design & Implementation-Volume 6 table of contents, 2004, pp. 10–10.

[20] Bardin, J"Security Guidance for Critical Areas of Focus in Cloud Computing," www. cloudsecurityalliance.org/ guidance/csaguide.pdf, 2009.

[21] Hwang, K G. Fox, and Dongarra.J, Distributed Systems and Cloud Computing: Clusters, Grids/P2P, and Internet Clouds, Morgan Kaufmann, to appear, 2010.
[22] Nick J, " Journey to the Private Cloud: Security and Compliance," tech. presentation, EMC, Tsinghua Univ., 25 May 2010.
[23] Rittinghouse J and Ransome.J, Cloud Computing: Implementation, Management and Security, CRC Publisher, 2010
[24] "Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner.com. Retrieved 2010-08-22.
[25] Ravi.V. and Shankar. R. (2005), Analysis of interactions among the barriers of reverse logistics, Technological Forecasting and Social Change, 72(8): 1011-1029.
[26] Thakkar. J.,Kanda.A. and Deshmukh, S.G. (2008), Interpretive Structural Modeling (ISM) of IT-enablers for Indian manufacturing SMEs', Information management & Computer Security, Vol. 16 No.2, pp. 113-136
[27] Quan Liu, Lu Gao, Ping Lou, "Resource Management Based on Multi-Agent Technology for Cloud Manufacturing, IEEE 2011
[28] Farzad Sabahi, " Cloud Computing Security Threats and Responses" IEEE, 2011.
[29] Craig A Lee, " A Perspective on Scientific Cloud Computing", ACM 2010
[30] P. Sasikala, " Cloud Computing: present status and the future implications", Inderscience Enterprises Ltd. 2011.