

TOTAL INTERPRETIVE STRUCTURAL MODELLING ON ENABLERS OF CLOUD COMPUTING

Ambikadevi Amma.T¹, N.Radhika², Pramod.V.R³

¹Research Scholar Karpagam University Coimbatore, TamilNadu

²Associate Professor, Computer Science & Engg Dept, Amrita vishwa vidyapeetham, Coimbatore, TamilNadu, India 641105

³Associate. Professor, Dept. of Mechanical Engineering, NSS College of Engg, Palakkad, Kerala, India 678008

Abstract

Cloud computing is the delivery of computer resources over a network through web services, while the actual physical location and organization of the equipment hosting these resources are unknown to the users. Cloud computing strategy is subjected to many enablers. Interpretive structural modeling is a well proven tool for finding the interrelationship among the enablers. Total Interpretive structural model is an essential innovative version of interpretive structural modeling technique (ISM). In Total Interpretive Structural Modeling (TISM), influence/enhancement of enablers and their interrelationship is considered. Total interpretive structural model steps are identification of elements, pair-wise comparison, level partition, interaction formation, digraph representation and formation of total interpretive structural model. The methodology of TISM is used to delineate the hierarchical relationship of enablers of cloud computing. Cloud computing is based on the concept of virtual machines. Hardware cost can be reduced by using virtualization. Different types of virtualization are operating system –level virtualization, application virtualization, service virtualization, memory virtualization, storage virtualization, virtual file system, data virtualization etc. Lack of trust between cloud users and providers has hindered the universal acceptance of cloud as outsourced computing services. To promote Multitenency we must design the cloud ecosystem to be secure, trustworthy and dependable

Keywords: cloud computing, enablers, partition levels, interaction matrix, TISM.

1. 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 hardware's and software's. 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 service providers provides the platform to the users any type of operating the systems along with hardware's & Software's.

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. 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-Service (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

Cloud computing is the delivery of computing as a service rather than a product, whereby information are provided to computers and other devices as a utility over a network. Cloud computing describes a new supplement, consumption, and delivery model for IT services based on internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. Cloud computing providers deliver application via the internet, which are accessed from a web browser.

2. LITERATURE SURVEY

Cloud computing is an emerging scenario of computing style where applications, data and resources are provided to users as services over the web. Consumers are not worried about the implementation of the cloud but they care about what the service does for them. Cloud computing provides configurable computing resources like servers, networks, storage and applications as and when required with minimum effort over the internet. The major critical success factor of cloud computing are consistent data availability and security. Data centre facility uses to house computer systems and associated components. It includes redundant power supply, data communication connections and security devices etc. Clouds are location independent providing abstract datacenter. Virtual servers, storage devices and networking are provided without human interaction. A consumer can provision computer facilities like server times and network storage. The cloud capabilities are available over the network and accessed through standard mechanisms like mobile phones, laptops and personal digital assistants. Using multitenant model the providers computing resources are pooled to serve multiple customers. The computing resources include storage, processing, memory, network bandwidth and virtual machines. Cloud capabilities can be rapidly, elastically and even automatically scaled out and rapidly released to quickly scale in. By leveraging a metering capacity at some level of abstraction, cloud systems automatically control and optimize resource use. Transparency is provided for both the provider and consumer regarding the resource usages. The resource usage is monitored, controlled and reported. Standardization and visualization are the keys to reduce infrastructure costs while meeting the dynamic needs of business.

Many organizations are migrating to cloud to derive flexibility and cost reduction benefits from their computing environment. Reasons why cloud computing is popular with business are cost factor, flexibility and service provisioning of the resources. Self service portal allows the clients to help themselves and makes the offering more available from a service perspective. Automation reduces IT operations costs. Cloud paradigm improves service delivery by applying engineering discipline and scale of economics in an internet inspired architecture.

Cloud deployment models are public cloud, private cloud and hybrid cloud. In public cloud the business rents and pay

for what they use on demand. In private cloud the service is on their organization network in its IT environments and delivers services to their users only. Hybrid cloud uses the combination of both public and private cloud. Public cloud services are available to customers from a third party service provider via the internet. Public clouds provide cost-effective means to deploy solutions. Companies can use it on demand and with the pay-as-you use policy.

Private clouds are deployment made inside the on-premise data centers and run by on site servers. Like public cloud private cloud offers cloud computing environment such as elastic on demand capacity, self service provisioning and service based access.

Hybrid cloud is a combination of interoperating public and private clouds. Hybrid models allow elasticity pay-as-you-go pricing, network isolation and secure connectivity just like privately owned data centre.

Cloud computing provides massively scalable computing resources from anywhere simplifies service delivery. It provides rapid innovation and dynamic platform for next generation datacenters. Use of virtualization and limited capabilities for monitoring access to applications hosted in the cloud. Data privacy is another factor concerning security. Quality of services like availability, reliability and performances are major security issues. No well defined service level agreements to meet standards. Integration and interoperability are also barriers to cloud.

Some of the features of the cloud are discussed herewith. Self service is one of the important features of the cloud. Using role-based access control it separates authenticated end-users. Dynamic workload management enables the datacenters with automation. Resource automation establishes secure Multitenancy and helps prevent contention in the load aware resource engine. Enabling the feature charge back, show back and metering the transparency in cloud business is attained. Cloud is integrated with the products in the datacenter. It is possible to meter the cloud resource usage. Cloud supports most of the operating systems and is possible to vary hardware configuration. Role-based access administrations are used for providing secure Multitenancy and bring security to the self-service cloud portal.

3. METHODOLOGY

ISM is an interpretive methodology goes as the judgment of the group decides the relationship of different elements in the system. An overall structure is extracted from the set of elements hence it is structural in the basis of mutual relationships and the overall structure are portrayed in a diagram model hence it is a modeling technique. Total ISM is also following some of the steps of ISM. Reachability and partition levels are adopted as it is in the process of TISM. It is having a step by step process and is briefly outlined below.

3.1 Step I: Elements Identification and Definition

First step in any structural modeling is to identify the elements whose relationship is to be modeled. For this

purpose the enablers of cloud computing are identified from literature survey and discussions with domain experts and is shown in table1.

Table 1: Major enablers of cloud computing and their definitions

Enabler Number	Major enabler of cloud computing	Definition
1	Data protection	Data available in cloud should be protected from external attacks.
2	Confidentiality	All datas should have authentication and authorization for protection also encryption.
3	Data integrity	Data should not be changed in an unauthorized manner.
4	Data availability	Data should be available to support the operations.
5	Multitenency	Sharing of resources across a large pool of customers.
6	Operational efficiency	Efficiency of operation depends on the interfaces, web connection and availability of data.
7	Elasticity	Application can expand and contract on demand.
8	Interoperability	Provision to operate different clouds in different countries.
9	Authorization	To manage user accounts and various assurance.
10	Auditing	Control based on defined principles and criteria for security, availability, confidentiality, integrity and privacy
11	Guidance	Handling identity and access management
12	Standards	Standards are defined by governing body or a market lead. It scarce as cloud is concerned.
13	Data lineage	Mapping application data flows or data path visualization.
14	Data remenance	The residual representation of data that has been in some way erased or removed.
15	Data provenance	Data has integrity and computationally accurate.

3.2 Step II: Contextual Relationship Definition

Model of the structure is developed by relating the elements. The contextual relationship between different elements are identified for the study is depicted in table1. for example the contextual relationship between different enablers for study is enabler1 will influence/enhance enabler2 etc. Experts' opinion is solicited to capture the contextual relationship among the elements.

3.3 Step III Relationship Interpretation

This step forwarded over the traditional ISM. Contextual relationship in ISM remains silent on how that relationship really works. In TISM explanation of how the enablers influence /enhance with each other is considered. It also explain in what way they influence /enhance each other

3.4 Step IV: Pair-Wise Comparison

A pair-wise comparison of elements is used to develop SSIM (Structured self interaction matrix.) in formal ISM. This interpretation indicates direction of relationship only. TISM make use of the concept by answering the interpretive query in step III for each paired comparison first element should be compared to all the elements in the row .For each comparison the entry should be Yes (Y) or No (N).The reason for yes should be provided. Comparing all the row elements a paired relationship in the form of interpretive logic –knowledge base is obtained Table2.

Table 2: Interpretive logic-knowledgebase

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N	N
2	Y	Y	N	Y	N	Y	Y	N	N	N	N	N	N	N	N
3	Y	Y	Y	Y	N	Y	Y	N	Y	N	N	N	N	N	N
4	Y	Y	Y	Y	N	Y	Y	N	N	N	N	N	N	N	N
5	Y	N	Y	Y	Y	Y	Y	Y	N	N	Y	Y	N	N	N
6	Y	N	N	N	N	Y	N	Y	N	N	Y	Y	N	N	N
7	Y	N	Y	Y	N	Y	Y	Y	N	N	N	N	N	N	N
8	Y	Y	N	N	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
9	N	Y	N	Y	N	N	N	N	Y	Y	Y	N	N	N	N
10	N	Y	N	N	N	N	N	N	Y	Y	Y	N	N	N	N
11	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
12	N	N	Y	Y	N	N	Y	Y	N	N	Y	Y	N	N	N
13	N	Y	N	N	N	N	N	N	Y	Y	Y	N	Y	Y	Y
14	N	N	N	N	N	N	N	N	Y	Y	Y	N	N	Y	Y
15	N	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y

3.5 Step V: Reachability Matrix and Transitivity

Check

Corresponding to Y in the knowledge base cell is replaced by 1 and N is replaced by 0. Check for transitivity and reachability matrix is shown in Table 3.

Table 3: Initial Reachability matrix

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

3.6 Step VI: Level Partition in Reachability Matrix

ISM based level partition is carried out. Reachability set and antecedent sets for all the elements are determined. Intersection of the two sets is found out. The elements for which the reachability set and intersection set are same occupy the top level in ISM hierarchy. Top level elements will not influence the remaining elements hence it can be removed from further calculation. The same process is

repeated until the levels of each element is found out. Level partition is shown in Table 4.

Table 4: 1ST Level partition

Enablers	Reachability set	Antecedent set	Intersection	Level
1	1,2,3,4,6,7,8,9,10,11	1,2,3,4,5,6,7,8	1,2,3,4,6,7,8	
2	1,2,4,6,7	1,2,3,4,8,9,10,13	1,2,4	
3	1,2,3,4,6,7,9	1,3,4,5,7,12	1,3,4,7	
4	1,2,3,4,6,7	1,2,3,4,5,7,9,12	1,2,3,4,7	
5	1,3,4,5,6,7,8,11,12	5,8	5,8	
6	1,6,8,11,12	1,2,3,4,5,6,7,8	1,6,8,12	
7	1,3,4,6,7,8,12	1,2,3,4,5,7,8,12	1,3,4,7,8,12	
8	1,2,5,6,7,8,9,11,12	1,5,6,7,8,12	1,5,6,7,8,12	
9	2,4,9,10,11	1,9,10,13,14,15	9,10	
10	2,9,10,11	1,9,10,13,14,15	9,10	
11	11	1,5,6,8,9,10,11,12,13,14	11	1
12	3,4,7,8,11,12	5,6,7,8,12	7,8,12	
13	2,9,10,11,13,14,15	13,14,15	13,15	
14	9,10,11,14,15	13,14,15	14,15	
15	10,13,14,15	13,14,15	13,14,15	

Table 5: levels of enablers

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

3.7 Step VII: Diagraph Development

The elements are arranged graphically in levels and links are drawn as per the relationship. Diagraph is used to represent the elements and their interdependence in terms of nodes and edges. The elements are arranged graphically in levels

and the directed links are drawn as per the relationship shown in reachability matrix. It is shown in Figure 1.

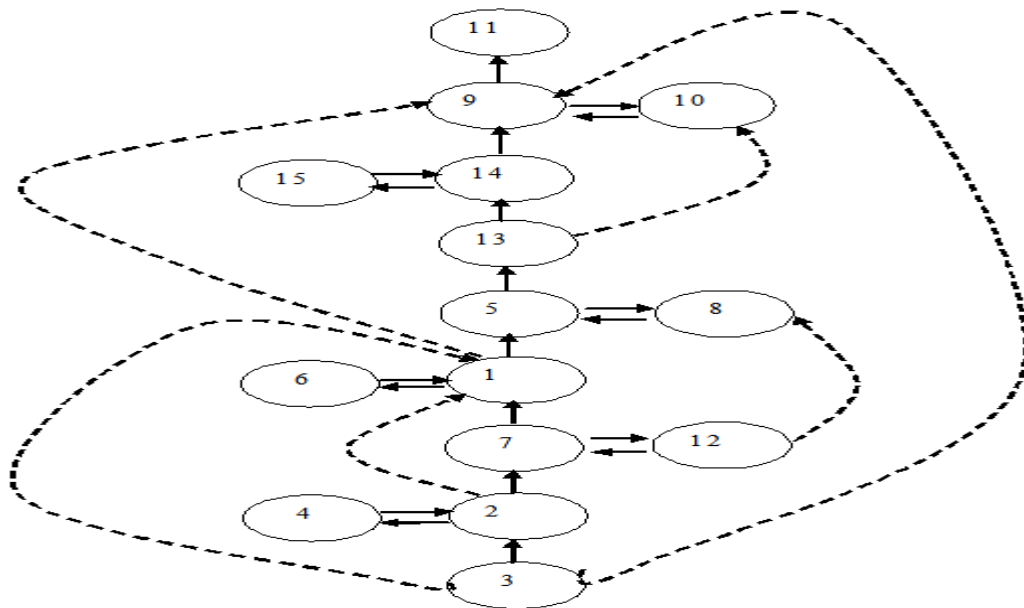


Fig 1 Diagram with significant transitive links

3.8 Step VIII: Interaction Matrix

The final diagram is translated into a binary interaction matrix form depicting all the interactions by 1 in cells. Remaining cells entry is 0. Cells with entry 1 are interpreted by picking the relevant interpretation from the knowledge

base in the form of interpretation matrix. The interaction matrix is shown in Table 6. and explanation is following the matrix representation

Table 6: Interaction Matrix

	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15
E1	1	0	0	0	1	1	0	0	1	0	0	0	0	0	0
E2	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0
E3	1	1	1	0	0	0	0	0	1	0	0	0	0	0	0
E4	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0
E5	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0
E6	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0
E7	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0
E8	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
E9	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0
E10	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0
E11	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
E12	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0
E13	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
E14	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1
E15	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

E1-E5- Multitenency means same data is pooled among a pool of users. Data protection is Important in the sense the pooled data should be accurate I all means.

E1-E6- Operational efficiency depends on data protection. Data is to be stored securely in the cloud. Therefore cloud service can be increased by increasing operational efficiency.

E1-E9- Authorizations in the sense, only privileged customers are directed to use cloud. Data can be protected

by providing security measures using cryptographical methods.

E2-E4- Data availability to customers depends upon protected data. Cloud services can be improved by providing datas availability.

E2-E7- Elasticity, means datas can be increased and decreased as per the users

E3-E1- Data integrity means data should remain without any change in the original data. This can be done if and only if data is protected securely.

E3-E2- Data for consumers should remain in the original form. Confidentiality of approach of cloud may improve if data integrity is preserved.

E3-E9- By providing authorization the data integrity can be preserved.

E4-E2- Data searching in cloud database must be available for the user thereby increasing the confidentiality level of the users.

E5-E8- Multiple users are able to use the same data from the pool of data. Interoperability of the system can be improved by Multitenancy

E5-E13- mapping of data depends upon data availability.

E6-E1- Operational efficiency is directly proportional to the data protection cloud. Efficiency can be increased by protecting data in cloud. Consumers may have very good opinion of the data so many are forced to use the cloud thereby increasing the efficiency.

E7-E1- the data using can be increased or decreased depending on users view. Elasticity can be applied if and only if clouds data is protected.

E7-E12- Common standard in cloud is necessary since the clouds operation is from different countries.

E8-E5- Interoperability among different clouds may affect Multitenency.

E9-E10- The hacking can be prevented by giving protection using authorization.

E9-E11- Guidance can be improved by improving authorization.

E10-E9- Auditing can be improved by using authorization.

E12-E7- Common standard for cloud will definitely improve elasticity.

E13-E14- Data reminance depends upon data lineage.

E14-E9- Data reminance depends on data auditing

E14-E15- Data prominence and data reminance are related to each other

E15-E14- . The residue of the data and the data computationally correct depends each other.

3.9 Step IX: Total Interpretive Structural Model

The information contained in the interpretive matrix and diagram are used to obtain TISM

The nodes are replaced with boxes containing elements. Interpretation is depicted on the side of the links. The total interpretive structural model is shown in Figure 2.

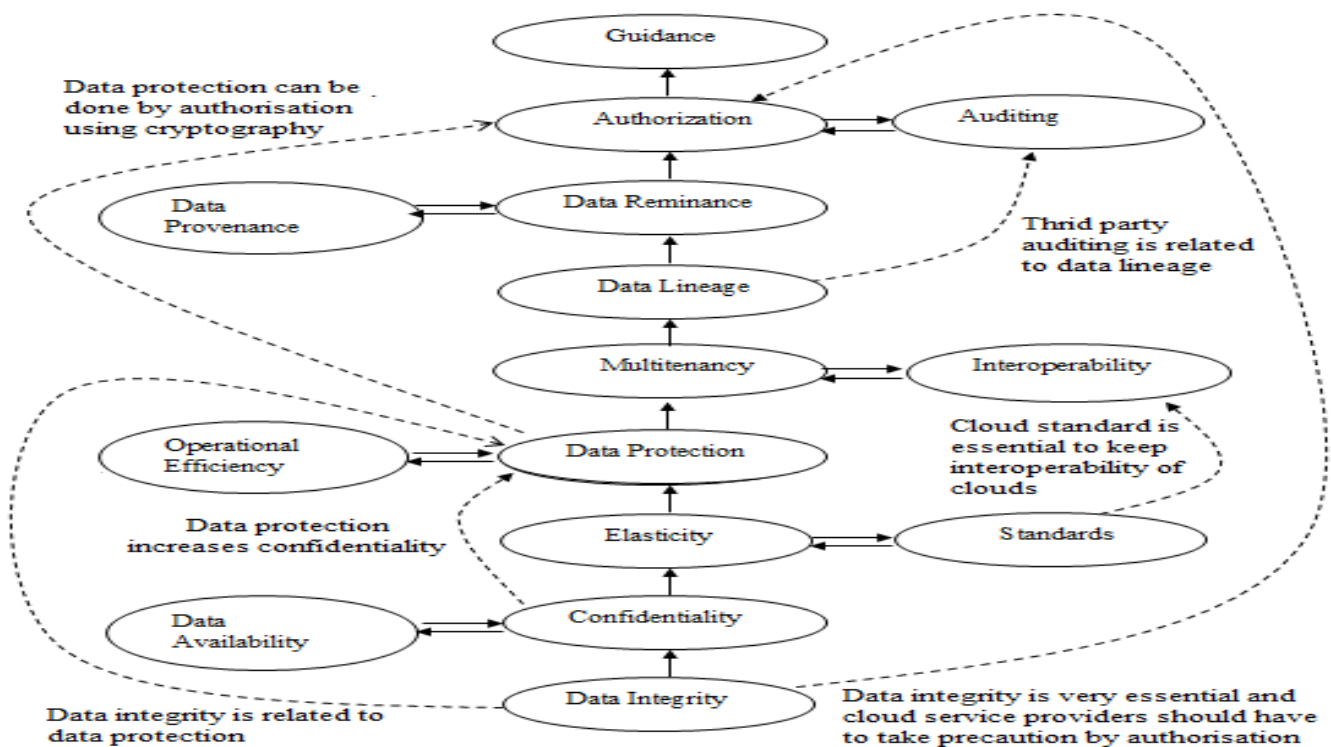


Fig 2: Total Interpretive Structural Model

4. RESULTS AND DISCUSSIONS

Inhibitors are put in different levels, so as to get the interrelationship of inhibitors. Level partition is done by considering reachability set, antecedent set and intersection set as described in the section. There are nine Partition levels. The elements coming under each level is discussed below. The inter relationship of enablers are found out. From the diagraph, guidance is first level element i.e. The top most element. Removal of the top most elements will not affect the system. The second level elements are authorization and auditing. Third level element data provenance and data reminance. Data lineage is coming under fourth level. Multitenency and inter operability are in the fifth level. Data protection and operational efficiency are in sixth level. Standards and elasticity are coming under seventh level. Data availability and confidentiality are coming under eight levels. Data integrity is in ninth level. Interrelationship among them is also shown in the Figure no. 1. Data integrity is very essential and cloud service providers should have to take precautions for data integrity. Data integrity is directly related to confidentiality and data availability. Confidentiality has an indirect relation to data protection. Standards are related to interoperability. The reason is that if all cloud service providers are having same standards then the operation on cloud become very easy. Data protected in cloud means data integrity is preserved. So they are related to each other. Operational efficiency depends on the availability of data. If all the datas are available operational efficiency can be increased. Data protection can be done by considering authorization. Authorization can be done by giving password protection and by providing cryptographic protection. Data lineage means mapping of data's and visualization of data. Data lineage is very important for auditors' assurance. So it is related to auditing. Confidentiality can be increased by proper authorization. In the sense protection of data by using password and cryptography.

5. CONCLUSIONS

Enablers of cloud computing are studied and their interrelationship is figured out. Total interpretive structural modeling is used. Difference between ISM and TISM is that in TISM the interpretation and logic behind the expressed relation is clarified where as in ISM no such clarification is given. Relationship of the inhibitors is shown in diagraph. Clarification in TISM may be through the experts. Contextual relationship in SSIM remains silent in ISM whereas in TISM the real working is considered. TISM of enablers of cloud computing is drawn and the relationship is explained in interaction matrix. Data integrity, data availability, data security, confidentiality, operational efficiency, standards, authorization .interoperability are coming as major enablers. Major enablers should be considered before going for cloud installation. Confidentiality and data protection are related to each other. Elasticity is depending on standards and standard can enhance interoperability proper standard will entertain the cloud computing services hence the Data lineage

dependence on data auditing. The reason is that data consumed or used can be audited by third party auditors.

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]. Attri R., Grover S., Dev N. and Kumar D., An ISM approach for modelling the enablers in the implementation of TotalProductive Maintenance (TPM), International Journal SystemAssurance Engineering andManagement,DOI:10.1007/s13198-012-0088-7 (2012)
- [12]. Warfield.J. Developing interconnection matrices in structural modeling. IEEE Transactionson Systems, Man and Cybernetics, 2005, 4(1): 81-67.
- [13]. Attri R., Grover S., Dev N. and Kumar D., Analysis ofbarriers of Total Productive Maintenance (TPM),International Journal System Assurance Engineering andManagement, DOI: 10.1007/s13198-012-0122-9 (2012)
- [14]. Raj T. and Attri R., Quantifying barriers to implementingTotal Quality Management (TQM), European Journal of Industrial Engineering, 4(3), 308-335 (2010)
- [15]. Ravi.V. and Shankar. R. (2005), Analysis of interactions among the barriers of reverse logistics, Technological Forecasting and Social Change, 72(8): 1011-1029.
- [16]. 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
- [17]. Quan Liu, Lu Gao, Ping Lou, "Resource Management Based on Multi-Agent Technology for Cloud Manufacturing, IEEE 2011
- [17]. Farzad Sabahi, " Cloud Computing Security Threats

and Responses” IEEE, 2011.

[18]. Craig A Lee, “ A Perspective on Scientific Cloud Computing”, ACM 2010

[19]. P. Sasikala, “ Cloud Computing: present status and the future implications”, Inderscience Enterprises Ltd. 2011