Journal of Policy Research, 9(1), 221-236.
https://jprpk.com
https://doi.org/10.5281/zenodo.7908753

Structural Analysis of the Barriers to Address Cyber Security Challenges

Abdul Basit[1], Tehmina Fiaz Qazi[2], Abdul Aziz Khan Niazi[3], Ifra Aziz Khan Niazi[4]

Abstract

The study is aimed to analyze the barriers to address the cyber security challenges. Research design includes examination of literature, data collection and analysis. It uses Interpretive Structural Modeling (ISM) technique with Matriced' Impacts Croise's Multiplication Appliquée a UN Classement (MICMAC). It is a qualitative approach to structure poorly articulated relations of elements of complex systems. Results of literature review show that there are total 18 barriers to address cyber security challenges. ISM generated a four level model i.e. barriers namely: 'collaborative barriers', 'data management', 'performance barriers', 'costs associated cyber threats and vulnerabilities', 'lack of documented processes', 'inappropriate cyber security policies', 'cyber terrorism', 'system migration vulnerabilities', 'complex operating system updates' and 'under-enforced cyber security policies' at top level; 'legal complication' at bottom level; remaining barriers at middle of model. Legal complication is the most critical barrier to address cyber security challenges. Barriers occupying middle part of model having moderate criticalness accordingly that on top have less criticalness. MICMAC analysis shows that 'legal complications' is independent whereas 'system migration vulnerabilities' is dependent, remaining all sixteen barriers are linking and no barrier is autonomous. The study has impactful practical implications for: internet service providers who can understand barriers and take informed decisions to plug the loops/incorporate counter solutions/checks; software vendors who can understand complex relations among barriers and create better built-in security checks; industry/companies across economy who understand barriers and better formulate corporate policies to prevent data and systems; individual users who will become well aware of issues of era of digitization; research community by way of providing theoretical framework for future researches. It also has implications for governments who can better understand cyber-security issues and formulate better policies, fool proof cyber-law, codes for criminal and civil matters concerning the cyber-security. This study will also help governments to prioritize the key barriers/issues and to handle with order of preference. It provides foundations for designing quantitative studies testing hypothesized mediation and/or moderation. It also has theoretical implications by extending the frontiers of knowledge and information about the phenomenon of cyber-security. The study also has some methodological, data and resources limitations. Methodological limitations include: qualitative with inductive approach in the era of quantitative approaches, answering what is related to what without cause and quantification, dispensing with transitive links in model and using majority rule contrary to consensus for aggregation. Data limitations include: review of limited amount of literature, collection of data from relatively small number of respondents (medium size of panel of experts), taking data on matrix questionnaire containing large number of pairs of relations by simultaneous evaluation. Limitations of resources include: limited time and lack of any financial support. It is an original study since it is conducted in real time field setting addressing highly practical angles of a unique topic in a simple but a novel way. It uses original data, well established methods, techniques and procedures and contributes new knowledge towards the domain in form of structural model, classification of barriers and related information. It is useful for internet service providers, software vendors, industry/companies across economy, individual users, governments and research community.

***Keywords**:* Cyber security challenges, ISM, MICMAC, barriers, cyber security

1. Introduction

In this era of information technology and digitization, large amount of data of systemic importance is being concurrently and continuously generated by computers/computing machines. That is inherently being stored on small portable/non-portable electronic gadgets. Safety of the data, storage and utilization has become something extremely important to be ensured. In this context, the effort is being made at different levels i.e. individual level, organizational level, government level, international level and intellectual level. Cybersecurity is important because it protects data of systemic importance from theft, damage, destruction or misuse. Data may be personal information, intellectual property related, government information and industry secrets. It may be sensitive and important for internet service providers, software vendors, industry/companies across economy, individual users, governments and research community (Fischer-Hübner et al., 2021). The researchers have unconditionally come forward to highlight and to solve the issues of cyber security and to formulate policy and/or technical guidelines to be disseminated for the

[1] Lahore Institute of Science & Technology, Lahore, Pakistan
[2] Hailey College of Banking and Finance, University of the Punjab, Lahore, Pakistan
[3] Corresponding Author, Institute of Business & Management, University of Engineering and Technology, Lahore, Pakistan
[4] Faculty of Management Studies, UCP Business School, University of Central Punjab, Lahore, Pakistan

stakeholders. For example: Venter (2014) argued that numerous new security challenges in recent paradigm shift towards virtualization in the cloud are sprouting that should be addressed. Lallie and Shepherd (2020) asserted that the cyber security attacks increased during COVID- 19 pandemic period and their modus-operandi has changed and frequency of attacks also changed in this period. Gunes (2020) revealed that cyber-attacks are new danger for critical infrastructures now a day, especially where the cyber physical systems are used. Akiyama et al. (2017) pointed out that i) IP-flux and domain-flux are concurrently used for deploying the intermediate sites of redirect chains to ensure robustness of redirection, ii) click fraud has become another motivation for attackers to employ URL redirection and iii) use of web-based domain generation algorithms has also become popular as a means to increase the entropy of redirect URLs to thwart URL blacklisting. Wang (2020) emphasized on thorough investigation of transformation of cybercrime industry from low-tech cyber-enabled crimes to high-tech sophisticated breaches. It asserted that viruses, worms/Trojan infections, electronic spam mails and hacking are the top most breaches. Almost every country has a large number of internet users that depends on an increased digitized security apparatus and on good internet connectivity. Laws are being promulgated to tackle threats of cyber-attacks in depth and wholesomeness, but still, there are number of challenges to ensure cybersecurity that need to be addressed immediately (Fischer-Hübner et al., 2021; Ali, 2022). Mammoth research on cyber security is found but hindrances to ensure security still exist. Why could the barriers not properly have addressed to date? is a research worthy question. Comprehensive list of barriers/hindrances could hardly be found and the way to address these barriers is rarely studied. Formal identification, structuring, categorization and prioritization of the barriers/hindrances missing part of contemporary literature. Since research on phenomenon is scanty and cybersecurity challenges are becoming complex day by day, therefore to understand the structure of barriers for managing cyber-security is a real time problem that is prevalent as threat to the systems of the stakeholders. Therefore, objectives this study are: prepare a list of barriers to address the challenges of cyber security, to a develop a structural model of complex relations among barriers, to analyze the relations, to classify them for simplification and discuss findings qua reality. Issues of cybersecurity have been studies using wide variety of different methods viz: survey, experiment, case study, literature review, interview, document analysis, focus group, secondary data analysis, big data analytics, proof of concept with survey, diary study, participatory design, hazard matching, meta-analysis, quasi-experimental study and so on (Quayyum et al., 2021; Audi et al., 2022). There are plenty of methodological choices available for doing this as well research and analysis but mostly involve deterministic mathematical/statistical models. We are afraid that the deterministic models may not support our scheme of study. A theory building approach of ISM with MICMAC is the best available option (Warfield, 1974) to achieve the above-mentioned objectives. It is commonly used to address this type of complex issues e.g. Rajan, et al. (2021): Majumdar, Garg, & Jain, (2021); Zeinalnezhad et al., (2021)**;** He, & Chen, (2021); Menon & Ravi (2021) and James et al., (2020); Audi et al., (2019). It is a well-established methodology for identification, modeling and summarization of relationships among multitude of systemic variables. It progresses stepwise and scientifically develops as structural model. Remaining study is arranged as the review of contemporary literature, methodology & analysis, results and conclusion.

2. Context and Review of Contemporary Literature

The study started with literature review since it establishes authors' understanding and knowledge the subject. It sets very outset of the study and demonstrates that how current study fits in the contemporary body of knowledge. It also expounds the resources explored by the authors. As an attempt to survey literature we explored the research databases namely: Frontiers, Elsevier (Science Direct), MDPI, Emerald, Cogent, Springer link, Hindawi, IEEE, Karger, Taylor & Francis, PLOS, Wiley-Blackwell using Google as search engine. Keywords for search include cybersecurity, cyber security, cybercrimes, cybersecurity management, barriers in cyber security management, challenges of cybersecurity, barriers to address cyber security challenges etc. Lot of research is found on cyber security concerning cyber security issues, cyber security endurance and cyber security attacks. Considerable literature is reviewed by the authors and some of the studies necessary to build the context of the study are parsimoniously reported in this section. Na Liu (2020) identified six major elements that could impact acceptance and ultimately adoption such as: user & vendor education, awareness, responsibility, safety, trust and legislation. Chamikara et al. (2016) proposed a new data perturbation algorithm called Secure and Efficient data perturbation Algorithm utilizing Local differential privacy (SEAL) that provides a good balance between privacy and utility with high efficiency and scalability. It argued that empirical comparisons with existing privacy-preserving algorithms show that SEAL excels in execution scalability, speed, accuracy and attack resistance. Johnson Cobb (2018) buttressed that recruiting more women into cyber-security is a win-win situation. They are stable, exciting and make cutting-edge career path with projected growth and businesses can benefit from a much-needed source of skilled talent to stay ahead of cyber-attackers. Kim (2014) identified a unique relationship between the companies that develop systems and their clients. It further found a hierarchical integration aspect of the relationship between IT developers and their clients. Amin M. Amin (2016) proposed a new methodology to prevent/detect hardware Trojans in third party IPs. It revealed higher probability of Trojan detection over a naive implementation of simple voting on the output of different IPs. Butavicius (2020) stated that stakeholders demonstrate general distrust of technical controls in order to enhance people’s ability to detect phishing emails. Chejerla (2013) argued that fusion architecture can detect collaborative attacks and profile them with high degree of accuracy to protect computer applications. Alguliyev (2018) emphasized on the impact of cyber threats on confidentiality, authenticity, reliability, integrity and resilience that is reflected as threats on actuators, sensor devices, communications, computing components and feedback. Chang (2019) concluded that cyber terrorism can be overcome by strengthening cyber security capacity and awareness. Shannon Eggers (2020) analyzed the supply chain threats and vulnerabilities that are often overlooked in cyber supply chain risk analysis. It proposed a novel supply chain cyber-attack surface diagram to assist with enumeration of risks and to examine the complex issues for securing firmware, hardware, software and system information. Chaturvedi (2013) hierarchicalized the issues related to cyber security and provide managerial insights for information security at national and organizational levels.

Table 1: List of Barriers to Address Cyber Security Challenges

Code	Barriers	Description	Source
1	Legal complexities	Constitutional and legal barriers preventing firms from sharing information about cyber threats and vulnerabilities.	(Koepke, 2017) (Biswas, 2020
2	Technological issues	Technological barriers include a lack of interoperability or compatibility between the sharing organization.	(Koepke, 2017)
3	Firms inability to secure too much information	Too much shared information and a firm’s inability to process this data being significant barrier.	Butavicius, 2020
4	Collaborative difficulties	Collaborative barriers include the challenges of establishing trust between a firm and sharing organization.	Chejerla, 2013
5	Data management issues	Management barriers involve challenges around the management of data and relationships from the firm and cyber information sharing organization perspectives.	Shannon Eggers, 2020
6	Absence of mechanisms	Organizational barriers to share information include firm’s inability to use data due to limited resources, and an absence of mechanisms to govern and control the use of sensitive information.	Chaturvedi, 2013
7	Performance impediments	Performance barriers include reputational damage and a loss of customers or revenue that yields a negative impact on a firm’s performance, thereby impeding future sharing.	(Koepke, 2017
8	Costs associated with cyber threats and vulnerabilities	The costs associated with sharing information about cyber threats and vulnerabilities often being significant barrier.	(Conteh & Schmick, 2016)
9	Lack of sufficient funding	Non-appropriation or in-sufficient appropriation of funds by the stakeholders to address cybersecurity challenges.	(Karakoç, 2017); Fischer-Hübner et al., 2021
10	Inadequate availability of cyber security professionals	Short supply of cyber security professional to understand and address cybersecurity challenges.	(Karakoç, 2017)
11	Increasing sophistication of cyber threats	The barriers to understand and address increasing sophistication of different types of cyber-attacks, threats and modus-operandi.	Alguliyev, 2018; Gunes, 2020
12	Lack of visibility of influence on enterprise	Lack of visibility of influence of the cyber security threats on the enterprise.	Amin M. Amin, 2016
13	Lack of documented processes	Lack of documented processes to implement cyber security management systems to circumvent cyber security challenges.	Na Liu, 2020
14	Inappropriate cyber security policies	Inappropriate or insufficient cyber security policy(ies) to circumvent cyber security challenges.	Adu, 2017)
15	Cyber terrorism	Politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.	(Wirtz & Weyerer, 2017); Mileski, 2018
16	System migration vulnerabilities	A system migration is the process of transferring business process or IT resources to a newer hardware infrastructure or a different software platform for the purpose of keeping up with current technologies and/or to gain better business value. This has become vulnerable due to increased cyber-attacks.	(Conteh & Schmick, 2016)
17	Complex operating system updates	An operating system is system software that manages computer hardware, software resources and provides common services for computer programs. This is becoming complex day by day.	Post & Kagan, 2003)
18	Under-enforced cyber security policies	Failure of policy enforcement is the activity of some members of government who act in an organized manner to enforce policy by discovering, deterring, rehabilitating or punishing people who violate the rules and regulations.	Suggested by Experts

Adu (2017) proclaimed that corporations have a good knowledge of IT but their awareness of cyber security is very limited. Goel (2019) developed a framework for cybersecurity risk assessment (known as PRISM framework) to identify and operationalize a tailored approach to address cyber security problems. Biswas (2020) revealed that technical measures and legal consequences are the most important antecedents for enhanced cyber-security levels in the organizations. Mileski (2018) found inconsistent information that may be the result of strength of power with which an artificial intelligence system is transmitted. Paul Sallos (2019) asserted that a knowledge-based perspective necessarily serves as the platform for a phenomenon-based view of organizational cyber security. From careful perusal of aforementioned short representation of research studies, inter alia, mammoth research literature of cyber security, a list of barriers to address the security challenges is extracted (Table 1).

Initially a list of seventeen factors is prepared and presented to the panel of experts for soliciting their opinion about relevance, sufficiency and accuracy of the factors. Majority of the experts is agreeable to all seventeen factors and at the same time they suggested to add one more barrier 'under-enforced cyber security policies' listed at serial 18 in Table 1. Building an ISM study on total eighteen factors is ideal.

3. Methodology/Data Collection/Analysis

Interpretivism approach is considered appropriate as research philosophy for this study. That is a qualitative inductive approach of structural modeling based on in-depth analysis. Literature review, data collection and in-depth analysis is the research design. People responsible for cyber security management are population under study. Focus group (panel of experts) is sampling technique. Data has been collected by the way of field survey by using VAXO based matrix type questionnaire (Niazi et al., 2019; Alawamleh & Popplewell, 2011), face-to-face, one-on-one (Shaukat, et al. 2021; Ali, 2022) data elicitation technique is used for extraction of data from the minds of respondents following the model exchange isomorphism approach. Interpretive Structural Modeling (ISM) is used to generate a structural model of complex relations among the barriers and MICMAC analysis is used to corroborate the results of ISM, validate model (Abbas et al. 2021), classify and analyze the barriers.

3.1. Panel of Experts

Source of data use for analysis and modeling is experts. Elicitation in this way is required when data are not-existing, expensive, limited or unreliable. In this case, data are considered as limited and/or unreliable. Therefore, focus group (panel of experts) is recruited with an assumption that their opinions are valid. Panel of experts consisting of 7 to 8 experts being heterogeneous in nature and 12 to 25 being homogeneous in nature is considered appropriate to build ISM based studies (Clayton, 1997; Khan & Khan, 2013). Experts outperform statistical groups as for as in-depth analysis is concerned (Clayton, 1997). On bases of a predetermined criteria a panel of experts is therefore recruited for collection of data. Criteria for selection of experts is based on the principle "quality is more important than quantity". Pakistan is facing numerous issue (Ali, 2022) and all the experts have the relevant theoretical, practical and empirical experience. Panel 16 experts is constituted that includes: one professor having number of research publications on cyber security management in impact factor journals, from large public sector university of Pakistan, two heads of IT of large public sector universities of Pakistan, one in charge computer lab/IT lab of one of the leading public sector business schools, one chief executive (PhD in computer science with number of publications concerning cyber security) of a medium sized international software house of Pakistan, one professor having experience and exposure of teaching cyber security management in a large private sector university of Pakistan and ten IT experts responsible for cyber security management from industry having masters level university education in information technology and/or computer science.

Table 2: Structural Self-Interaction Matrix (SSIM)

Code	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1		V	V	V	O	V	V	V	V	O	V	O	V	A	V	V	V	V
2			V	V	A	V	V	V	V	V	V	O	O	A	V	V	A	V
3				V	V	V	A	V	A	A	V	V	A	V	V	O	V	O
4					V	V	A	V	V	V	V	A	V	O	V	O	V	A
5						V	V	V	A	A	V	V	A	V	V	V	A	A
6							V	O	V	A	V	O	V	A	O	V	O	V
7								V	A	X	V	A	V	V	V	V	A	A
8									V	V	V	V	O	A	V	V	A	A
9										V	A	O	O	O	V	V	V	V
10											V	A	V	V	V	V	V	V
11												A	V	V	V	V	V	V
12													O	V	V	V	V	O
13														A	A	V	A	X
14															O	V	V	X
15																X	V	V
16																	O	V
17																		O
18																		

Table 3: Binary Matrix (Direct Reachability)

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

Table 4: Transitive Binary Matrix

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

Experts on panel were approached face-to-face one-on-one basis in office setting four times. One for introducing the study and inviting them to participate and developing the rapport; secondly for verification of factors; third time for data elicitation; fourth time for model checking and verification. It took us more than three to four months to complete the process from developing rapport to development of model. Authors had different options/choices to collect the data like: Delphi method, different type of interviews, Nominal Group Technique (NGT), matrix type questionnaire, one-to-one, face-to-face in-depth interview, approval voting on alternatives, etc. Data are elicited from the experts on a matrix type VAXO based questionnaire commonly used for ISM based studies. Data are collected on *ij* part only, while during the process of rapport development and invitation, number of rounds of discussions are made with experts on panel. Each of the response is separately fed in MS Excel and aggregate (majority response) on every paired relation of *ij* part is attained using the 'count-if function' of MS Excel applying the principle "minority gives way to majority" (Li, et al. 2019; Abdullah & Siraj, 2014).

3.2. Proceeding to ISM Process

Following the classical approach of ISM as proposed by Warfield (1973) we applied stepwise procedure. As a first step we obtained SSIM (Structural Self Interaction Matrix) as a result of aggregation of responses abovementioned.

SSIM is converted into initial reachability matrix using classical procedure of binary coding devised by Warfield (1973) and iterated by Attri, Dev & Sharma (2013).

All zeros (0s) in initial reachability matrix are checked for transitivity using certain functions of MS Excel and attained fully transitive matrix namely final reachability matrix (Table 4).

By way of checking and incorporating transitivity as above mentioned, some of the zeros (0s) are replaced with 1* because of transitive relations. The transitive binary matrix is then partitioned into levels by using classical iteration method (Table 5-8).

Table 5: Iteration I

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

Table 6: Iteration II

Code	Reachability Set	Antecedent Set	Intersection Set	Level
1	1,2,3,6,9,10,11,12	1,3,10,11,12	1,3,10,11,12	
2	2,3,6,9,10,11,12	1,2,3,9,10,11,12	2,3,9,10,11,12	
3	1,2,3,6,9,10,11,12	1,2,3,6,9,10,11,12	1,2,3,6,9,10,11,12	*II*
6	3,6,9,10,11	1,2,3,6,9,10,11,12	3,6,9,10,11	*II*
9	2,3,6,9,10,11,12	1,2,3,6,9,10,11,12	2,3,6,9,10,11,12	*II*
10	1,2,3,6,9,10,11,12	1,2,3,6,9,10,11,12	1,2,3,6,9,10,11,12	*II*
11	1,2,3,6,9,10,11	1,2,3,6,9,10,11,12	1,2,3,6,9,10,11	*II*
12	1,2,3,6,9,10,11,12	1,2,3,9,10,12	1,2,3,9,10,12	

Table 7: Iteration III

Code	Reachability Set	Antecedent Set	Intersection Set	Level
1	1,2,12	1,12	1,12	
2	2,12	1,2,12	2,12	*III*
12	1,2,12	1,2,12	1,2,12	*III*

Table 8: Iteration IV

Code	Reachability Set	Antecedent Set	Intersection Set	Level
1	1	1	1	*IV*

Using the permutation mehtod, a conical matrix is prepared to extract structural model on diagonals (Table 9). All the ISM process is captured into a one comprehensive but condensed representation (Table 10).

Table 9: Conical Matrix

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

Table 10: Condensed Representation of ISM

Reachability Sets

Antecedent Sets	**Level**	**Code**	**4**	**5**	**7**	**8**	**13**	**14**	**15**	**16**	**17**	**18**	**3**	**6**	**9**	**10**	**11**	**2**	**12**	**1**	Driving Power
	Level I	**4**	1	1	1*	1	1	1*	1	1*	1	1*	1*	1	1	1	1	1*	1*	0	**17**
		5	1*	1	1	1	1*	1	1	1	1*	1*	1*	1	1*	1*	1	1	1	1*	**18**
		7	1	1*	1	1	1	1	1	1	1*	1*	1	1*	1*	1	1	1*	1*	1*	**18**
		8	1*	1*	1*	1	1*	1*	1	1	1*	1*	1*	1*	1	1	1	0	1	0	**16**
		13	1*	1	1*	1*	1	1*	1*	1	1*	1	1	1*	0	0	1*	1*	1*	0	**15**
		14	1*	1*	1*	1	1	1	1*	1	1	1	1*	1	1*	1*	1*	1	1*	1	**18**
		15	1*	1*	1*	1*	1	1*	1	1	1	1	1*	0	0	0	0	1*	0	0	**12**
		16	1*	1*	1*	1*	1*	1*	1	1	1*	1	0	0	0	0	0	0	0	0	**10**
		17	1*	1	1	1	1	1*	1*	1*	1	1*	1*	1*	1*	1*	1*	1	1*	0	**17**
		18	1	1	1	1	1	1	1*	1*	1*	1	1*	1*	1*	1*	1*	1*	1*	1*	**18**
	Level II	**3**	1	1	1*	1	1*	1	1	1*	1	1*	1	1	1*	1*	1	1*	1	1*	**18**
		6	1*	1*	1	1*	1	1*	1*	1	1*	1	1*	1	1	1*	1	0	0	0	**15**
		9	1*	1	1	1*	1*	1*	1	1	1	1	1	1*	1	1	1*	1*	1*	0	**17**
		10	1*	1	1	1*	1	1	1	1	1	1	1	1	1*	1	1	1*	1*	1*	**18**
		11	1*	1*	1*	1*	1	1	1	1	1	1	1*	1*	1	1*	1	1*	0	1*	**17**
	Level III	**2**	1	1*	1	1	1*	1*	1	1	1*	1	1	1	1	1	1	1	1*	0	**17**
		12	1	1*	1	1*	1*	1	1	1	1	1*	1*	1*	1*	1	1	1*	1	1*	**18**
	Level IV	**1**	1	1*	1	1	1	1*	1	1	1	1	1	1	1	1*	1	1	1*	1	**18**
			18	**18**	**18**	**18**	**18**	**18**	**18**	**18**	**18**	**18**	**17**	**16**	**15**	**15**	**16**	**15**	**14**	**9**	

Dependence Power

3.3. Establishing ISM Model

The model extracted in conical matrix highlighted as grey is converted into digraph and that being the optional step of ISM (Sushel, 2012) is not reported here to maintain brevity. The digraph is converted into a structural model by labeling barrier descriptions along-with codes duly connected with arrows corresponding the inter barrier relationships. The model is also divided into sub-sections for making its representation simpler (Figure 1).

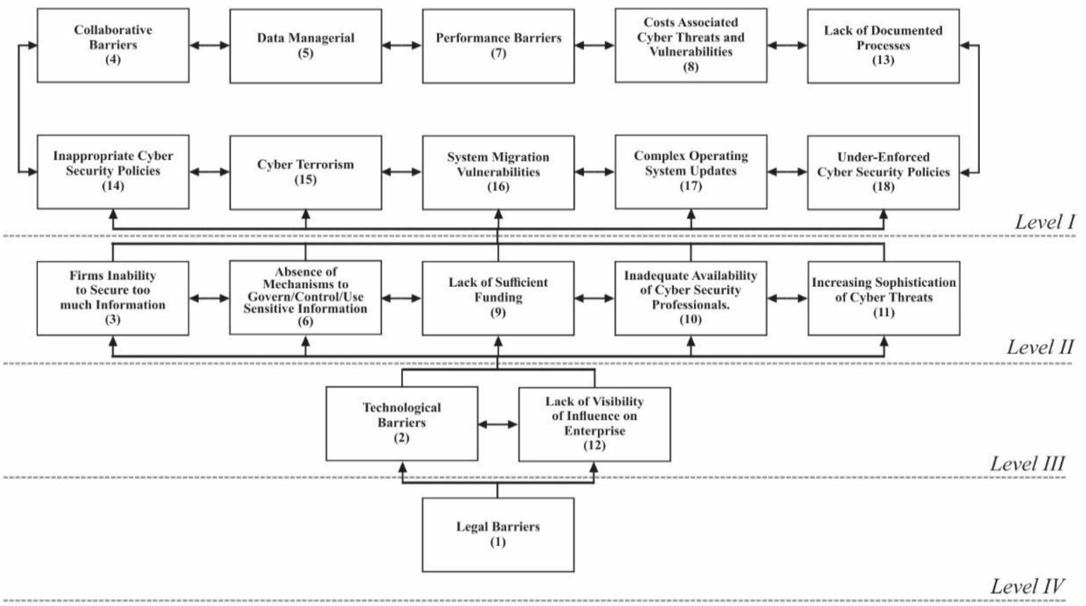
Collaborative Barriers (4)
Data Managerial (5)
Performance Barriers (7)
Costs Associated Cyber Threats and Vulnerabilities (8)
Lack of Documented Processes (13)
Inappropriate Cyber Security Policies (14)
Cyber Terrorism (15)
System Migration Vulnerabilities (16)
Complex Operating System Updates (17)
Under-Enforced Cyber Security Policies (18)
Level I
Firms Inability to Secure too much Information (3)
Absence of Mechanisms to Govern/Control/Use Sensitive Information (6)
Lack of Sufficient Funding (9)
Inadequate Availability of Cyber Security Professionals. (10)
Increasing Sophistication of Cyber Threats (11)
Level II
Technological Barriers (2)
Lack of Visibility of Influence on Enterprise (12)
Level III
Legal Barriers (1)
Level IV

Figure 1: ISM Model

Close observation of the model depicts that 10 barriers fall at *Level I* coded as*:* 4, 5, 7, 8, 13, 14, 15, 16, 17 & 18. Similarly, 5 factors fall at *Level II* coded as*:* 3, 6, 9, 10 & 11. Further, 2 factors fall on *Level III* coded as*:* 2 & 12. Only one factor falls at *Level IV* coded as*:* 1.

3.4. MICMAC Analysis

Model derived as a result of ISM process and placement of factors at different levels is corroborated and verified by further analysis i.e. MICMAC analysis (Godet, 1986) analysis (Figure 2).

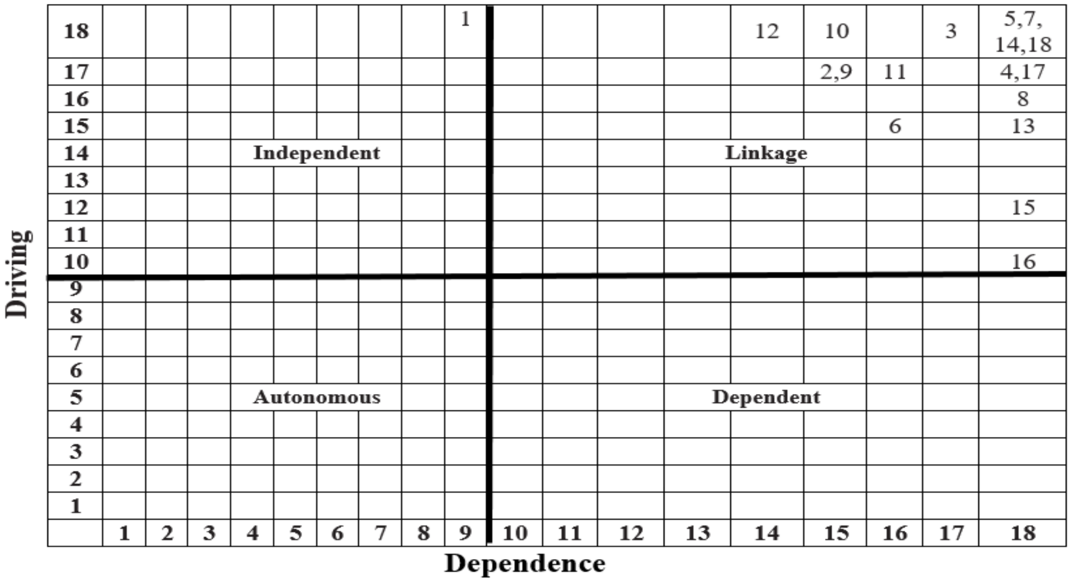

Figure 2: Driving-Dependence Diagram

Barriers are categorized under four classes using scale centric approach. Under *Autonomous* quadrant, no factor lies that means all barriers under study are relevant to the phenomenon under study. Under *Independent* quadrant, only one factor falls i.e., 1. Under *Dependent* quadrant, only one barrier falls that is 16. All the remaining barriers (i.e. barriers coded as 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17 & 18) fall under quadrant *Linkage* that means that these barriers are agile, unbalanced, unsettled or ambivalent.

4. Results

With the aim of identifying, prioritizing, structuring, analyzing and classifying the barriers the study used literature review and ISM with MICMAC. The results of literature review show that there are 18 barriers contributing towards need to investigated for addressing the cyber security challenges. Findings of the study show that: total ten barriers namely 'collaborative barriers (4)'; 'data management (5)'; 'performance barriers (7)'; 'costs associated cyber threats and vulnerabilities (8)'; 'lack of documented processes (13)'; 'in-appropriate cyber security policies (14)'; 'cyber terrorism (15)'; 'system migration vulnerabilities (16)'; 'complex operating system updates (17)'; 'under-enforced cyber security policies (18)' fall at *Level I*. Similarly, five barriers namely 'firm's inability to secure too much information (3)'; 'absence of mechanisms to govern/control/use sensitive information (6)'; 'lack of sufficient funding (9)'; 'inadequate availability of cyber security professionals (10)'; 'increasing sophistication of cyber threats (11)' fall at *Level II*. Further, two barriers 'technological barriers (2)'; 'lack of visibility of influence on enterprise (12)' fall at *Level III*. Only one barrier 'legal barriers (1)' falls at *Level IV*. Corresponding to Figure 2, all barriers are categorized into four classes using scale centric MICMAC analysis that shows under autonomous quadrant, no factor lies, under independent quadrant, only one barrier namely 'legal barriers (1)' falls, under dependent quadrant, only one barrier namely 'system migration vulnerabilities (16)' fall. All remaining barriers namely 'collaborative barriers (4)'; 'data management (5)'; 'performance barriers (7)'; 'costs associated cyber threats and vulnerabilities (8)'; 'lack of documented processes (13)'; 'inappropriate cyber security policies (14)'; 'cyber terrorism (15)'; 'complex operating system updates (17)'; 'under-enforced cyber security policies (18)'; 'firm's inability to secure too much information (3)'; 'absence of mechanisms to govern/control/use sensitive information (6)'; 'lack of sufficient funding (9)'; 'inadequate availability of cyber security professionals (10)'; 'increasing sophistication of cyber threats (11)'; 'technological barriers (2)'; 'lack of visibility of influence on enterprise (12)' fall under quadrant linkage. The results aforementioned are abridged (Table 11).

Table 11: Results Juxtaposed

Result of Literature Review		Results of MICMAC Analysis				Results of ISM	Comments
Code	Issue	Driving	Dependence	Effectiveness	Cluster	Level	
1	*Legal complexities*	*18*	*9*	*9*	*Independent*	*IV*	*Key factor*
2	Technological issues	17	15	2	Linkage	*III*	
3	Firms inability to secure too much information	18	17	1	Linkage	*II*	
4	Collaborative difficulties	17	18	-1	Linkage	*I*	
5	Data management issues	18	18	0	Linkage	*I*	
6	Absence of mechanisms	15	16	-1	Linkage	*II*	
7	Performance impediments	18	18	0	Linkage	*1*	
8	Costs associated with cyber threats and vulnerabilities	16	18	-2	Linkage	*1*	
9	Lack of sufficient funding	17	15	2	Linkage	*II*	
10	Inadequate availability of cyber security professionals	18	15	3	Linkage	*II*	
11	Increasing sophistication of cyber threats	17	16	1	Linkage	*II*	
12	Lack of visibility of influence on enterprise	18	14	4	Linkage	*III*	
13	Lack of documented processes	15	18	-3	Linkage	*I*	
14	Inappropriate cyber security policies	18	18	0	Linkage	*I*	
15	Cyber terrorism	12	18	-6	Linkage	*I*	
16	System migration vulnerabilities	10	18	-8	Dependent	*I*	
17	Complex operating system updates	17	18	-1	Linkage	*I*	
18	Under-enforced cyber security policies	18	18	0	Linkage	*I*	

The juxtapose results of both of the techniques (ISM and MICMAC) well enlighten upon the driving and dependence power of the barriers and set the priorities by way of hierarchy and/or alignment. The barrier highlighted as grey in Table 11 is a key barrier that is evident as a result of the technique of modeling as well as that of analysis.

5. Discussion

This study explores barriers and relations among barriers to address cyber security challenges. It generated a list of barriers, applied ISM and MICMAC as methodology that is an approach altogether different from traditional mathematical algorithms. It generated different results and that are important to be discussed in order enrich understanding of readers from different perspectives. Discussion is divided into five sub-parts: i) discussion on results of the study, ii) discussion on contrasting the study with contemporary literature, iii) discussion on implications of the study, iv) discussion on limitations of the study and v) discussion on recommendations for future research studies to overcome the limitations of current study.

5.1. Discussion on results of the study

The results of review of literature are considered appropriate since the barriers are generated from valid literature sources and are also verified by the panel of experts. According to norms of ISM based studies 18 variable are sufficient to represent any phenomenon under study. As for as results of ISM method are concerned the model of four levels has the capability to give sufficient insight. The hierarchy of the model considering the bottom to top approach prioritizes the barriers according the importance. It is indicative of the most important barrier (key barrier or barrier occupying bottom of the model) to deal with at policy level that is capable of driving all rest. Moderators/mediators are also captured on model (middle of the model). Barriers of least criticalness also surged to occupy top of the model. Therefore, ISM model means a lot to discerners. The results of the model are also corroborated by the results of MICMAC. MICMAC analysis divides the barriers into four categories in a scale of eighteen. Autonomous barriers mean the barriers that are not connected to the others and hence the need to be eliminated from the system and absence of the variables means that all the variable under study are relevant and important.

Table 12: Comparison of present study with prior ones

Sr.	Study	Country	Focus	Variables	Results	Method
1	Current	Pakistan	Barriers to address cyber security challenges.	18 barriers to address cyber security challenges	Legal complexities is key barrier	ISM with MICMAC analysis
2	Butavicius et al. (2020)	Autralia	Degree of trust in firewalls and anti-virus software.	-	Development of a 'trust in technical controls' scale for measuring people's faith in technical controls.	Multiple linear regression analysis along- with classical descriptive statistics.
3	Chaturvedi, et al. (2014)	India	To identify critical information security issues, create a framework and to provide interesting managerial insights about their hierarchy.	25 top information security issues and factors.	Cyber security at government level and cyber security treaties at international level.	Delphi method with ISM
4	Hart, et al. (2020)	UK	Cyber security awareness and education.	-	Concluded that tabletop games e.g. Riskio, increase cyber security awareness.	Experimental study designed on games for assessing learning.
5	Rajan et al., (2021).	India	Organizational strategic cybersecurity management	7 factors (i.e. resources and capabilities, information flow, training, alliance and collaboration, governance, security awareness and technological infrastructure)	Governance is the independent and key factor.	Modified Total Interpretive Structural Model (M-TISM)
6	Lallie et al. (2021)	UK	Cyber security cyber-attacks, analysis of cyber-crime and cybersecurity during the during COVID-19 pandemic.	Phishing, smashing, hacking, denial of service, malware, financial fraud, pharming, and extortion.	Highlighted a common modus-operandi of many cyber-attacks during this period.	Timeline methodology
7	Wilson, (2020)		Acceleration of digital transformation and cyber security.	-	Digitization without security is a recipe for disaster.	Theoretical paper.

Independent variables are those variable that have the capability of driving the others they have high driving power and low dependence power. In this study ‘legal complexities (1)’ is independent if we recall it also fall at bottom of ISM model being most important and powerful. Hence the results of ISM are validated. Dependent variables are those variables having high dependence but low driving power, in this, ‘system migration vulnerabilities (16)’ is dependent factor. This result is also aligned to ISM. Linkage variables are agile, unbalanced/unsettled or ambivalent. Except one independent and one dependent all are linking. Linking factors have high driving power and high dependence power and any action on them will in turn affect all other variables including themselves. Therefore, policy stakeholders should take actions on them with caution.

5.2. Discussion on contrasting the study with contemporary literature

This study has distinguishing features among the contemporary literature on many counts. The study covers relatively large number of variables (Table 1) and one can hardly find any other study envisaged on as many number of variables pertaining to cyber security. The study has some unique features like: simple heirarchalization and prioritization with relational model instead of complex algorithms etc. that distinguish it from within current literature. Contextually speaking, it is a unique attempt from within developing countries. It also has many aligning point with contemporary literature viz: it addresses the issue that is being studied all over the world from different perspectives, the results are in general aligned with overall literature though the depth of the study is different. It is not out of context to place the study in tabular form in contrast with some important studies of the domain (Table 12).

5.3. Discussion on implications of the study

Data of systemic importance is now stored on small electronic gadgets that has made it more vulnerable to cyber-attacks. Recognizing this fact now a day it has become highly relevant for all stakeholders of big data to understand different perspectives of cyber-security. Since this study deals an important aspect of cyber-security therefore it has serious implications for stakeholders. It has practical and theoretical implications that are discussed separately hereinafter.

Practical implications of the study: The study has lot of practical implications like:

- Practical implications for internet service providers: It is useful for internet service providers by way of developing their understanding on barriers to address challenges of cyber-security. They can take informed decisions to plug loops and incorporate counter solutions or checks to prevent the systems and/or data of their customers.
- Practical implications for software vendors: It is useful for software venders by way of developing their understanding about on cyber-security vulnerabilities and they can create better built-in security checks to prevent systems and data of their companies and customers.
- Practical implications for industry/companies across economy: It is useful for industry/companies across economy by way of developing their understanding about cyber-security vulnerabilities and they can better formulate the cyber security policies and can ensure better security checks to prevent their data and systems.
- Practical implications for individual users: It is useful for individuals by way of developing their understanding and awareness in general to build well informed society in the era of digitization.
- Practical implications for governments: The study is useful for governments and regulators by way of developing their understanding about cyber-security vulnerabilities. It will be helpful to them in formulating better policies, fool proof cyber-law, codes for criminal and/or civil matters concerning the cyber-security. This study will help them to prioritize the key barriers and issues for handling them with due order of preference. It will also help the government to set the future directions of cyber policy making.
- Practical implications for research community: The study provides theoretical framework for future researches. It provides foundations for designing the empirical quantitative studies that can test the phenomenon holistically or partially. The relations identified in ISM model can be hypothesized and tested statistically. Mediation/moderation studies can be designed using the information provided as a result of ISM/MICMAC analysis by way of testing hypotheses in deterministic models.
- Theoretical implications of the study: This research neither confirms nor refutes any theoretical premise but it extends the frontiers of knowledge and information about the phenomenon of cyber-security. It covers a range of barriers to address the challenges of cyber-security and put them in logical order. The order that is useful for the practitioners.

5.4. Discussion on limitations of the study

Limitations of the study may be discussed from three different angles i.e. methodological limitations, data limitations and resources limitations. As for as methodology is concerned, firstly, it is a qualitative methodology used with inductive approach that uses elementary concepts of Boolean algebra, set theory and directed graph theory therefore analytical strength is accordingly limited. Secondly, ISM method answers the question: What is related to what? and does not quantify the relations, does not tell cause and it also does not tell the pole of relationship. Thirdly, while constructing ISM model transitive links are removed and ignored for simplification. Fourthly, the responses are aggregated by using the majority rule (statistically saying mode value) instead of consensus. As for as data limitations are concerned, firstly, the data is collected from a medium size panel of experts from Pakistan only. Secondly, the matrix type questionnaire used for data collection that contains quite a numbers of pairs which is a difficult type of questionnaire that has the chance of stereo-typing. Thirdly, list of barriers is generated from a review of limited number of studies which is not claimed as exhaustive and there may be some other barrier that would have been included. Fourthly, the data have been collected using bi-valence (0, 1) that ignores fuzzy values. Fifthly, the data have been collected from Pakistani experts therefore the generalization of results is accordingly limited. As for as limitations of resources are concerned, firstly, it is collected in very limited time by the researcher professors by profession having lot of job commitments. Secondly, this is independent research and a non-funded study therefore it was constrained accordingly.

5.5. Discussion on recommendations for future research to overcome limitations of current study

This section formulates recommendations for future researchers to overcome the limitations aforementioned and enhance the frontiers of findings of the study. It is recommended that future studies should:

- use advanced quantitative methodologies like SEM, GMM, Wavelet analysis etc. in order to overcome the limitation of qualitative methodology,
- use T-ISM, Modified T-ISM, Polarized T-ISM etc. to overcome the limitations of quantification, cause and pole etc.
- use T-ISM, Modified T-ISM, Polarized T-ISM and include some important transitive links to overcome the limitation of removing transitive links,
- use Delphi method or some other method to create consensus in order to overcome limitations of majority rule,
- constitute optimum size of panel consisting of highly expert persons from some educationally and technologically advanced country in order to overcome the limitation of panel size, expertise of the experts on panel and context of the study,
- use logic-knowledge base questionnaire to overcome the limitations of matrix questionnaire,
- prepare an exhaustive list of barriers through rather thorough literature review to include all possible barriers,
- design studies using fuzzyISM/fuzzy-TISM/fuzzy-MICMAC etc. to construct a rather refined model, and
- design funded research study of international level envisaged over reasonable period of time and with the support of international institutions because it is issue of international concern.

5.6. Contribution of the study

The study contributed towards literature: i) a verified/refined list of barriers to address cyber security challenges, ii) ISM model, iii) MICMAC diagram, iv) information on driving/dependence power of each barrier (i.e. intra-model relationships) and v) discussion on model/analysis qua reality contrasting with contemporary literature.

6. Conclusion

Purposefulness of the research is to analyze the barriers to address cyber security challenges. Currently the world has embarked on IT based systems that are complex and vulnerable and subject to cyber threats. Cyber threats, mostly, prevail on cyber security management solutions. It is important to secure and protect information, resources, systems, and/or data that is vulnerable to cyber-crimes by listing the barriers which are hindrance to address cyber security challenges and then prioritizing them to get a clearer picture. Literature review, ISM along with MICMAC analysis is used to identify barriers, develop structure and analyze barriers. The results of literature review show that there are total 18 barriers contributing towards hindrances in cyber security challenges (Table 1). Findings of the study show that: total ten barriers namely ‘collaborative barriers (4)’; ‘data management (5)’; ‘performance barriers (7)’; ‘costs associated cyber threats and vulnerabilities (8)’; ‘lack of documented processes (13)’; ‘in-appropriate cyber security policies (14)’; ‘cyber terrorism (15)’; ‘system migration vulnerabilities (16)’; ‘complex operating system updates (17)’; ‘under-enforced cyber security policies (18)’ fall at *Level I*. Similarly, five barriers namely ‘firm’s inability to secure too much information (3)’; ‘absence of mechanisms to govern/control/use sensitive information (6)’; ‘lack of sufficient funding (9)’; ‘inadequate availability of cyber security professionals (10)’; ‘increasing sophistication of cyber threats (11)’ fall at *Level II*. Further, two barriers ‘technological barriers (2)’; ‘lack of visibility of influence on enterprise (12)’ fall at *Level III*. Only one barrier ‘legal barriers (1)’ falls at *Level IV*. Corresponding to Figure 2, all barriers are categorized into four classes using scale centric MICMAC analysis that shows under autonomous quadrant, no factor lies, under independent quadrant, only one barrier namely ‘legal barriers (1)’ falls, under dependent quadrant, only one barrier namely ‘system migration vulnerabilities (16)’ fall. All remaining barriers namely ‘collaborative barriers (4)’; ‘data management (5)’; ‘performance barriers (7)’; ‘costs associated cyber threats and vulnerabilities (8)’; ‘lack of documented processes (13)’; ‘inappropriate cyber security policies (14)’; ‘cyber terrorism

(15)'; 'complex operating system updates (17)'; 'under-enforced cyber security policies (18)'; 'firm's inability to secure too much information (3)'; 'absence of mechanisms to govern/control/use sensitive information (6)'; 'lack of sufficient funding (9)'; 'inadequate availability of cyber security professionals (10)'; 'increasing sophistication of cyber threats (11)'; 'technological barriers (2)'; 'lack of visibility of influence on enterprise (12)' fall under quadrant linkage. The study has impactful practical implications for: internet service providers who can understand barriers and take informed decisions to plug the loops/incorporate counter solutions/checks; software vendors who can understand complex relations among barriers and create better built-in security checks; industry/companies across economy who understand barriers and better formulate corporate policies to prevent data and systems; individual users who will become well aware of issues of era of digitization; research community by way of providing theoretical framework for future researches. It also has implications for governments who can better understand cyber-security issues and formulate better policies, fool proof cyber-law, codes for criminal and civil matters concerning the cyber-security. This study will also help governments to prioritize the key barriers/issues and to handle with order of preference. It provides foundations for designing quantitative studies testing hypothesized mediation and/or moderation. It also has theoretical implications by extending the frontiers of knowledge and information about the phenomenon of cyber-security. The study also has some methodological, data and resources limitations. Methodological limitations include: qualitative with inductive approach in the era of quantitative approaches, answering what is related to what without cause and quantification, dispensing with transitive links in model and using majority rule contrary to consensus for aggregation. Data limitations include: review of limited amount of literature, collection of data from relatively small number of respondents (medium size of panel of experts), taking data on matrix questionnaire containing large number of pairs of relations by simultaneous evaluation. Limitations of resources include: limited time and lack of any financial support.

References

Abbass, K., Niazi, A. A. K., Qazi, T. F., Basit, A., & Song, H. (2021). The aftermath of COVID-19 pandemic period: barriers in implementation of social distancing at workplace. *Library Hi Tech*.

Abdullah, M. R. T. L., & Siraj, S. (2014). Interpretive Structural Modeling of MLearning Curriculum Implementation Model of English Language Communication Skills for Undergraduates. *Turkish Online Journal of Educational Technology-TOJET*, *13*(1), 151-161.

Adu, K. K., & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *Foresight*, 20(2), 150-161.

Alawamleh, M., & Popplewell, K. (2011). Interpretive structural modelling of risk sources in a virtual organisation. *International Journal of Production Research*, *49*(20), 6041-6063.

Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*, 212-223.

Ali, A. (2022). Determining Pakistan's Financial Dependency: The Role of Financial Globalization and Corruption. *Journal of Business and Economic Options*.

Ali, A. (2022). Financial Liberalization, Institutional Quality and Economic Growth Nexus: Panel Analysis of African Countries, *Bulletin of Business and Economics*, 11(3), 37-49

Ali, A. (2022). Foreign Debt, Financial Stability, Exchange Rate Volatility and Economic Growth in South Asian Countries. *Journal of Business and Economic Options*.

Attri, R., Dev, N., & Sharma, V. (2013). Interpretive structural modelling (ISM) approach: an overview. *Research Journal of Management Sciences*, *2319*, 1171.

Audi, M., Ali, A. & Roussel, Y. (2019). The advancement in Information and Communication Technologies (ICT) and economic development: a panel analysis. *International Journal of Innovation, Creativity and Change*, 15(4), 1013-1039.

Audi, M., Ali, A., & Al-Masri, R. (2022). Determinants of Advancement in Information Communication Technologies and its Prospect under the role of Aggregate and Disaggregate Globalization. *Scientific Annals of Economics and Business*, *69*(2), 191-215.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cyber security: development of a trust in technical controls scale. *Computers & Security*, *98*, 102020.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cyber security: development of a trust in technical controls scale. *Computers & Security*, *98*, 102020.

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security*, *97*, 101959.

Chaturvedi, M., Singh, A. N., Gupta, M. P., & Bhattacharya, J. (2014). Analyses of issues of information security in Indian context. *Transforming Government: People, Process and Policy*, *8*(3), 374-397.

Chaturvedi, M., Singh, A. N., Gupta, M. P., & Bhattacharya, J. (2014). Analyses of issues of information security in Indian context. *Transforming Government: People, Process and Policy*, *8*(3), 374-397.

Choo, K. K. R., Abawajy, J., & Islam, R. (2017). Special issue on cybersecurity in the critical infrastructure: Advances and future directions. *Journal of Computer and System Sciences*, *83,* 1-2.

Clayton, M. J. (1997). Delphi: a technique to harness expert opinion for critical decision-making tasks in education. *Educational Psychology*, *17*(4), 373-386.

Cobb, M. J. (2018). Plugging the skills gap: The vital role that women should play in cyber-security. *Computer Fraud & Security*, *2018*(1), 5-8.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31.

Eggers, S. (2021). A novel approach for analyzing the nuclear supply chain cyber-attack surface. *Nuclear Engineering and Technology*, *53*(3), 879-887.

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., ... & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, *61*, 102916.

Godet, M. (1986). Introduction to la prospective: seven key ideas and one scenario method. *Futures*, *18*(2), 134-157.

Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. *Information & Computer Security*, *28*(4), 591-625.

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security*, *103*, 102196.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, 101827.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, 101827.

He, Z., & Chen, H. (2021). Critical factors for practicing sustainable construction projects in environmentally fragile regions based on interpretive structural modeling and cross-impact matrix multiplication applied to classification: A case study in China. *Sustainable Cities and Society*, *74*, 103238.

James, A. T., Kumar, G., Bhalla, M., Amar, M., & Jain, P. (2020). Analysis of challenges for automobile service garages in India: a structural modeling approach. *Journal of Advances in Management Research*. 18(3), 392-413.

Jones, K., Janicke, H., Maglaras, L., & Xenakis, C. (2020). Introduction to the special issue of the journal of information security and applications on" cyber security in ICS & SCADA systems". *Journal of Information Security and Applications, 54,* 102542.

Karakoç, M. (2017). *Understanding the barriers to addressing cybersecurity challenges in American state and local governments*. University of Delaware.

Khan, S., & Khan, M. S. A. (2013). Conceptualized Model of Green It Purchasing Enablers–An Application of Delphi Technique and Interpretive Structural Modeling. *Business Sciences International Research Journal*, 1(1), 24-37.

Kim, D. Y. (2014). Cyber security issues imposed on nuclear power plants. *Annals of Nuclear Energy*, *65*, 141-143.

Kim, K. C., & Im, I. (2014). Issues of cyber supply chain security in Korea. *Technovation*, *34*(7), 387-388.

Koepke, P. (2017). Cybersecurity information sharing incentives and barriers. *Sloan School of Management at MIT University*.

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2020). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*,

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Li, G., Huang, D., Sun, C., & Li, Y. (2019). Developing interpretive structural modeling based on factor analysis for the water-energy-food nexus conundrum. *Science of The Total Environment*, *651*, 309-322.

Liu, N., Nikitas, A., & Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation Research Part F: Traffic Psychology and Behaviour*, *75*, 66-86.

Majumdar, A., Garg, H., & Jain, R. (2021). Managing the barriers of Industry 4.0 adoption and implementation in textile and clothing industry: Interpretive structural model and triple helix framework. *Computers in Industry*, *125*, 103372.

Menon, R. R., & Ravi, V. (2021). Analysis of barriers of sustainable supply chain management in electronics industry: An interpretive structural modelling approach. *Cleaner and Responsible Consumption*, 100026.

Mileski, J., Clott, C., & Galvao, C. B. (2018). Cyberattacks on ships: a wicked problem approach. *Maritime Business Review*, *3*(4), 414-430.

Niazi, A. A. K., Qazi, T. F., & Basit, A. (2019). An Interpretive Structural Model of Barriers in Implementing Corporate Governance (CG) in Pakistan. *Global Regional Review*, 4(1) 359-375.

Osborn, E., & Simpson, A. (2017). On small-scale IT users' system architectures and cyber security: A UK case study. *Computers & Security*, *70*, 27-50.

Othmane, L. B., Jacobson, D., & Weippl, E. (2019). Special Issue on Security and Privacy in Smart Cyber-Physical Systems. *Computers & Security, 87*, 101611.

Post, G., & Kagan, A. (2003). Computer security and operating system updates. *Information and Software Technology*, *45*(8), 461-467.

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 100343.

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change*, *170*, 120872.

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change*, *170*, 120872.

Saadawi, T., & El-Desouki, A. (2014). Special issue on “Cyber Security”. *Journal of Advanced Research*, *5*(4), 413.

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, *20*(4), 581-597.

Shaukat, M. Z., Niazi, A. A. K., Qazi, T. F., & Basit, A. (2021). Analyzing the Underlying Structure of Online Teaching during the COVID-19 Pandemic Period: An Empirical Investigation of Issues of Students. *Frontiers in Psychology*, *12*, 605138. doi.org/10.3389/fpsyg.2021.605138

Singh, S., & Gupta, A. (2020). An ISM modeling for factors affecting the purchase of green products. *Journal of Modelling in Management*, 16(1), 103-123.

Sushil, A. (2017). Modified ISM/TISM Process with Simultaneous Transitivity Checks for Reduced Direct Pair Comparisons. *Global Journal of Flexible Systems Management*, *18*(4), 331-351.

Venter, H. S. (2014). Security issues in the security cyber supply chain in South Africa. *Technovation, 7*(34), 392-393.

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415.

Warfield, J. N. (1973). Binary matrices in system modeling. *IEEE Transactions on Systems, Man, and Cybernetics*, (5), 441-449.

Warfield, J. N. (1974). Toward interpretation of complex structural models. *IEEE Transactions on Systems, Man, and Cybernetics*, (5), 405-417.

Wilson, S. (2020). The pandemic, the acceleration of digital transformation and the impact on cyber security. *Computer Fraud & Security*, *2020*(12), 13-15.

Wilson, S. (2020). The pandemic, the acceleration of digital transformation and the impact on cyber security. *Computer Fraud & Security*, *2020*(12), 13-15.

Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and cyber-attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration*, *40*(13), 1085-1100.

Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, *77*, 103201.

Yang, S. H., Cao, Y., Wang, Y., Zhou, C., Yue, L., & Zhang, Y. (2021). Harmonizing safety and security risk analysis and prevention in cyber-physical systems. *Process Safety and Environmental Protection*, *148*, 1279-1291.

Zeinalnezhad, M., Chofreh, A. G., Goni, F. A., Hashemi, L. S., & Klemeš, J. J. (2021). A hybrid risk analysis model for wind farms using Coloured Petri Nets and interpretive structural modelling. *Energy*, *229*, 120696.

Annexure 1

Summarized Questionnaire

Barriers		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Legal complexities	■																	
2	Technological issues	▒	■																
3	Firms inability to secure too much information	▒	▒	■															
4	Collaborative difficulties	▒	▒	▒	■														
5	Data management issues	▒	▒	▒	▒	■													
6	Absence of mechanisms	▒	▒	▒	▒	▒	■												
7	Performance impediments	▒	▒	▒	▒	▒	▒	■											
8	Costs associated with cyber threats and vulnerabilities	▒	▒	▒	▒	▒	▒	▒	■										
9	Lack of sufficient funding	▒	▒	▒	▒	▒	▒	▒	▒	■									
10	Inadequate availability of cyber security professionals	▒	▒	▒	▒	▒	▒	▒	▒	▒	■								
11	Increasing sophistication of cyber threats	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	■							
12	Lack of visibility of influence on enterprise	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	■						
13	Lack of documented processes	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	■					
14	In appropriate cyber security policies	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	■				
15	Cyber terrorism	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	■			
16	System migration vulnerabilities	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	■		
17	Complex operating system updates	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	■	
18	Under-enforced cyber security policies	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	■