The Current State of Cyber-Readiness of Saudi Arabia

Nawaf Alhalafi [1] and Dr. Prakash Veeraraghavan [1],
17814379@student.ltu.edu.au P.Veera@latrobe.edu.au
La Trobe University, Computer Science & Information Technology Department.

Abstract

The continuous information technology and telecommunication (ICT) developments inspire several Saudi Arabia citizens to transact and interact online. However, when using online platforms, several people are likely to lose their personal information to cybercriminals. In the survey, 553 Saudi Arabia citizens and 103 information technology (IT) specialists confirm the expansion of digital economy and the need for smart cities with various services, including e-commerce and solid cyber security. 96.6% of the participants believe Saudi Arabia is digitalizing its economy; yet, 33.3% of the participants believe that residents are uninformed about living and operating in smart cities. Several people (47.29%) with medium internet speed are more aware about smart cities than those with fastest internet speed (34%). Besides, online transactions via credit cards subjected 55.5% of the participants to privacy and security issues. These findings validate the essence of cyber security awareness programs among Saudi Arabia citizens and IT professionals to boost public trust and acceptance of cybersecurity frameworks.

Keywords:
Cyber-readiness of Saudi Arabia, ICT, Information Technology, Cybersecurity Framework

Introduction

In recent years, several businesses have adopted digital and technological solutions to various operations, including leadership, communication, and transactions. The rapid growth and development of various technologies such as the internet, laptops, mobile phones, and personal computers have amplified human interconnectivity. As a result, several people and businesses are increasingly embracing virtual transactions, entailing cashless payment and online shopping and the percentage of users is likely to increase due to the rapid technological discoveries in various countries.

Different countries, including Saudi Arabia that have embraced digital economy are vulnerable to cyberattacks. In recent years, several nations such as the United States (US), Saudi Arabia, Singapore, and India have encountered the most disastrous cybercrimes. Interestingly, unlike other regions, more Saudi Arabia citizens are susceptible to various internet scams, including social media scams, bank fraud, and bank account hacking. Since several Saudi Arabians are concerned about cybersecurity, the country should boost its cyber security systems. This process is essential to improve citizen's trust and knowledge about how to improve and maintain their online security as they participate in the digital economic transformations, including working in smart cities. The study assesses factors influencing cybersecurity adoption in Saudi Arabia, including lack of trust on cybersecurity infrastructures, limited developments of cybersecurity frameworks, culture, and absence of trained IT experts.

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.36

1. Research Overview

1.1 Research Hypothesis

According to Chigbu (2019), a hypothesis can be considered a scientific tool for all kinds of qualitative study. It can be applied by qualitative researchers in varied ways. Hypothesis testing entails a process of exploring information to solve a specific issue linked to the problem under research. Whether a qualitative reviewer decides to test, validate, nullify, or approve a given phenomenon is a matter of semantics (Chigbu, 2019). Following an extensive literature assessment, researchers ought to state in clear terms the applicable hypotheses. Therefore, a hypothesis is a tentative presumption aimed at inferring and testing empirical results.

Considering the literature review, a framework to shape information systems (IS) governance is required for a country to have robust information security executions.

From the model applied, specific stakeholders within the four nations are tasked with certain IS governance responsibilities, which must be executed in synergy. Such roles must also be effective and relevant, which necessitates proper assessment for efficiency. Hence, the following hypotheses were drawn from the framework.

H_1. The lack of trust related to cyber infrastructure issues, services from governments or companies, cyber threats attacks, and cyber based economy limit cybersecurity frameworks adoption in Saudi Arabia.

H_2. The lack of developments related to shortage of cyber awareness programs and lack of trained personnel limit cybersecurity frameworks adoption in Saudi Arabia.

H_3. Cultural influences, including using of social apps and influence Saudi Arabia's adoption of cybersecurity awareness methods.

H_4. The lack of IT professionals in public sector (a shortage of local expertise) limits the implementation of cybersecurity frameworks in Saudi Arabia.

1. 1.2 Methodology:

One of the most significant parts of academic study is the research technique. It includes an in-depth examination of the technique employed to select the most effective and appropriate methods for carrying out the research. The design, involved techniques, data collection technologies, as well as data analysis used, as well as the strategies and approaches adopted, are also discussed in this part. Concerns about the study's validity and reliability are also addressed, with the purpose of ensuring that only proper and relevant information or data used to get findings. The methodology illustration is a way that aids in restricting research actions that might depart from the precise solution to identify study-related issues. The author could successfully and efficiently gather crucial data after developing the essential controls.

2. 1.3 Research Approach

The efficiency of the research strategy is determined as a study methodology's part. There are II sorts of research methodology in research: inductive and deductive research methods (Bengtsson, 2016). Determining the research approach is based on seeing the nature of the investigation, which illustrates that both methods are important. In a deductive research approach, the researcher establishes certain significant results by developing hypothesis statements depends on the study hypotheses. Inductive research, on the other hand, identifies a multitude of patterns related with the research's variables, as well as the observations created depends on the data patterns.

3. 1.4 Research Design

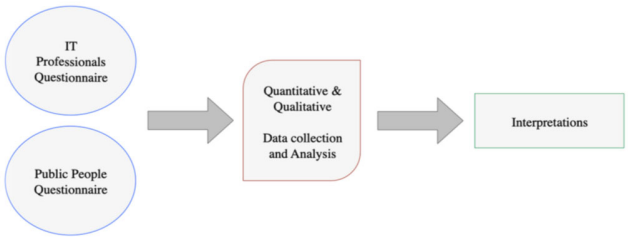

Fig. 3. Research design

There are three different research designs employed while carrying out a study: qualitative research, quantitative research, and mixed research (Palinkas et al., 2015). Quantitative research is based on the analysis of numerical numbers and quantities. This type of data is collected through surveys where questionnaire is used as a tool to gather the relevant information. Furthermore, data is acquired via utilising internet databases, online sources, and government-created websites. A qualitative research process is based on a knowledge of human prefers and behaviour to collect data from participants of the study in their natural surroundings (Wahyuni, 2012). The mixed research method, on the other hand, is a hybrid of both

methodologies. In this study, mixed method is employed to obtain the research findings.

The purpose of this study is to look at Saudi Arabia's cyber security situation and to promote the cyber security awareness program among IT users. The information was acquired from Saudi Arabian citizens and IT professionals to see how well they are aware of the cyber security community and whether they are in favor of supporting such initiatives in their nation. Another questionnaire was created for IT experts to learn about the state of ICT in Saudi Arabia and how effectively e-commerce is expanding there. The information was gathered from persons of various ages. The study also wants to discover if Saudi Arabian citizens desire to live in smart cities with all of the technological amenities such as e-commerce, solid cyber security, and digital marketing.

We have applied a cluster hypothesis over the study data in which we have the claim that the citizens of Saudi Arabia are aware of the cybersecurity, and they want to attend courses about this matter; they have the knowledge about the smart cities, and they are eager to live in that; they believe that by the development of the technology sector the lives will be easier. Further we have set the hypothesis according to the seniors in the tables shown in the results section.

Data analysis was conducted on Statistical Package for the Social Sciences (SPSS) version 20. All the categorical variables were presented in the form of n (%). The chi-square test of independence was used to observe the difference between groups and for the reliability test we use Cronbach's alpha. $P<0.05$ was considered statistically significant.

4. 2. Results and Analysis

Table: 1. Demographics of the study

IT PROFESSIONALS		
Gender		
Male	Female	Total (N)
73	30	103
IT industry experience		
	1 - 2 years	16 (15.2%)
	2 - 5 years	12 (11.4%)
	5 - 8 years	34(32.4%)
	8 - 10 years	17 (16.2%)
	10+ years	24(22.9%)
Qualification		
	Matriculation	9 (8.6%)
	Intermediate	57 (54.3%)
	Graduation	33 (31.4%)
	Postgraduate	2 (1.9%)
	M. Phil	2 (1.9%)
Profession		
	IT sector	52 (49.5%)
	Educational sector	18 (17.1%)
	Construction sector	8 (7.6%)
	Food sector	25 (23.8%)
PUBLIC SURVEY		
Gender		
Male	Female	Total (N)
348	206	554

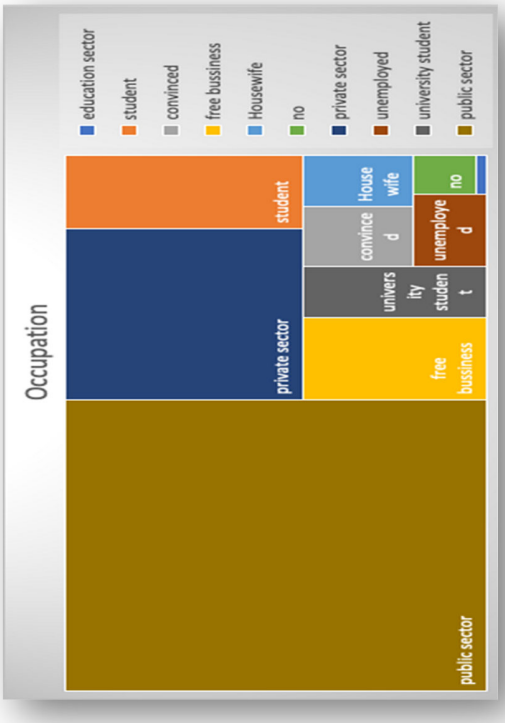

Figure 4. Profession of the public survey participants.

In the above graph we observed that there are big percent of public sector and private sector participants, participated in this study. Most of the participants of this survey belong to public sector.

2.1 LACK OF TRUST

2.1.1 Cyber Infrastructure:

Cyber infrastructure refers to the availability of IT facilities to connect the data fetching, transfer among all users. The following analysis depicts the perceptions of the participants about availability and usage of cyber infrastructure.

Table: 2. Cyber security platform in Saudi Arabia and capacity to design in smart cities

Variable	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Does Saudi Arabia have good cyber security platform?	1 (1%)	2 (1.9%)	20 (19%)	45 (42.9%)	35 (33.3%)
How strongly believe we have knowledge and capacity to design and deploy smart cities?	0	5 (4.8%)	31 (29.5%)	32 (30.5%)	35 (33.3%)

The above table shows that Saudi Arabia need to improve its cyber security platform. As 42.9% of the population strongly disagree with this statement. Citizen of Saudi Arabia may face threats in the form of internet scams, WhatsApp links, hack bank account, bank fraud, and social media scams. This is the clear evidence that Saudi citizens have no trust on cyber security platforms.

The above table shows that participants of the study does not believe that Saudi Arabia has enough knowledge and capacity to allocate smart city facilities. 33.3% participants strongly expressed their concerns about the capacity to run smart cities. They have also shown lack of knowledge of capacity to adopt and live-in smart cities.

2.1.2 Saudi Arabia's Adoption towards Digital Economy

Technology has transformed to become an integral part of modern economy. The "digital economy" comprises completely digital areas, including ICT and conventional sectors affected by digitalization. As a primary lever to realize its vision 2030 objective of diversifying the

economy, the Kingdom of Saudi Arabia (KSA) is taking resolute actions towards digital transformation (Little 3). In this view, the National Digital Transformation Unit was established to coordinate efforts across industries and monitoring the general progress of digital transformation in the country. It is estimated that the digital economy in Saudi Arabia contributed over 17% GDP in 2020 and is anticipated to exceed 19% by 2025 (Little 3). KSA enhanced the quality of digital services offered to beneficiaries by collaborating with the private sector to deliver fiber-optic network coverage to over 3.5 million homes across the country, escalating internet traffic during the COVID-19 pandemic by 30% (GOV.SA). In addition, internet traffic through the Saudi Arabian Internet Exchange (SAIX) was doubled, with internet speed growing from 9Mbps in 2017 to 109 Mbps in 2020 (GOV.SA). Overall, the government has provided comprehensive support for digital transformation as part of Vision 2030.

Table: 3. Saudi Arabia's growing digital economy

Variables	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Rate how much Saudi Arabia is moving towards digital economy ?	71 (67.6%)	25(23.8%)	4 (3.8%)	3 (2.9%)	0

According to the results of table 3, it has been seen that yes Saudi Arabia is moving towards digital economy i.e. 67.6% of the people are strongly agree and 23% are agree. This reflects the tendency of the people to wards digital economy.

Table: 4. Participant's awareness about various IT issues

Variable	Frequency
Email scam	2 (1.94%)
Bank fraud	5 (4.85%)
Social media scam	30(29.12%)
Viruses (that can lose the personal information from the workplace)	15 (14.56%)
Mobile data	14 (13.59%)
Fake Advertisements (job advertisement, links on social media, advertisement messages)	20 (19.41%)
External threats	8 (7.76%)
Fake accounts or hackers	9 (8.73%)

The above table shows that participants have sufficient information above social media scams i.e., 29.1% ranked the social media issues at the top. 19.4% people think fake advertisements as the second most important IT related issues, while 15% consider viruses as the 3rd important IT related issue. We may conclude that majority of the participants consider social media scams, fake advertisement, and viruses as the most important concerns that they may face while using IT infrastructures.

Table: 5. Trust and continuity competition base parameters

Variable	Frequency
Information leakage	23 (22.33%)
Hacking bank accounts	22(21.35%)
Unprofessional work environment	27 (26.21%)
Improper Cyber security system	31 (30.09%)

Above table shows that the citizens consider that improper cyber security system (30.09%) is the major parameter of lack of trust on cyber infrastructure following unprofessional work environment (27%).

2.1.3 Internet Speed and Use of Smart Devices:

The participants from general public were asked to evaluate their internet speed and their connected smart devices. The following sub-hypothesis was framed to test the responses statistically using regression analysis.

H0: Fast speed of internet having no influence over the awareness of smart devices.

H1: Fast speed of internet having no influence over the awareness of smart devices.

Table: 6. Use of smart devices based on internet speed in Saudi Arabia

		Are you aware of your internet-connected smart devices at home?		Total	P-value
		No	Yes		
How do you rate your current Internet speed?	Fast	5 (13.88%)	178 (34.36%)	183	0.047
	Medium	22 (61.11%)	245 (47.29%)	267	
	Slow	9 (25%)	74 (14.28%)	83	
	Very fast	0(0%)	21 (4.05%)	21	

The above table is set to the hypothesis that the internet speed have the influence over the awareness of smart devices in which we comes to that people having the fastest speed having the less percentage (34%) whereas the people having the medium speed having the higher percentage which is (47.29%) so it shows that the awareness or knowledge about the smart devices is not depending upon the internet speed they had it is about the matter of interest the p-value is significant thus we reject the null hypothesis. We may elaborate that the speed of internet and connectivity of smart devices is significantly associated with each other.

2.1.4 Digital Economy and use of E-commerce:

E-commerce has revolutionized the business and services sector during the recent years globally. The following sub-hypothesis was set to test the relationship between digital economy and e-commerce.

H0: They didn't know about digital economy and didn't make much online shopping and transactions.

H1: They know about digital economy and made much online shopping and transactions.

			Have you ever made any transactions online (e.g. paying an online bill, shopping, etc.)?			P-value
			I do not know	No	Yes	
Female	Do you know about digital economy?	I don't care	0	0	3 (1.59%)	0.551
		No	1 (100%)	4 (23.52%)	53 (28.19%)	
		Yes	0	13 (76.47%)	132 (70.21%)	
	Total		1	17	188	
Male	Do you know about digital economy?	I don't care	0	2 (16.66%)	9 (2.70%)	0.000
		No	1 (33.3%)	6 (50%)	43 (12.91%	
		Yes	2 (66.6%)	4 (33.3%)	281(84.38%)	
	Total		3	12	333	

Table: 7. Use of e-commerce by the participants and digital economy

In table 7 we have observed that both male and female respondent are aware of the digital economy, and they are making online transactions and online shopping etc. The percentage in female (70.21%) and in males (84.38%) which is quite a high percentage showing that they have the knowledge, and they are making online transactions whereas the p-value is found to be non-significant in females and significant in males. This means that males are

aware of digital economy, and they are significantly involved in e-commerce while female are reluctant to adopt e-commerce.

2.1.5 Credit Card Frauds and Cybersecurity:

With the use and adoption of e-commerce the digital payments have been common to secure the buyer and seller. The customers often use their credit cards for payments; however, they may face some frauds due to cybersecurity issues. The following hypothesis demonstrates the relationship between the cybersecurity and frauds while using credit cards.

H0: security issues and credit card fraud happened frequently.

H1: Not having security issues and credit card fraud happened frequently.

Table 8: cyber security concerns due to credit cards use and frauds

			Have you had any problems with breaching security/privacy?			P- value
			I haven't had problems breaching security/privacy, and I'm not worried about these issues.	I haven't had problems breaching security/privacy, but I worry about these issues.	I've recently had problems breaching security/breaching privacy, and I'm concerned about these issues.	
Female	Has your card been subjected to any fraud?	I don't know	1 (2.94%)	6 (4%)	1 (4.54%)	0.031
		No	33 (97.05%)	138 (92%)	17 (77.27%	
		Yes	0	6 (4%)	4 (18.18%)	
	Total		34	150	22	
Male	Has your card been subjected to any fraud?	I don't know	4 (8%)	12 (76%)	3 (6.52%)	0.000
		No	41 (82%)	206 (81.74%)	20 (43.47%)	
		Yes	5 (10%)	34 (13.49%)	23 (50%)	
	Total		50	252	46	

In table no.8 we observed that the female respondents having less percentage of facing fraud and problems of security and privacy which is like (18.18%) however the results are found to be significant and in males the percentage is higher which (50%) of the respondents have been in the issue of fraud and they are going through the problem of security and privacy thus the p-value is significant, so we accept the alternative hypothesis which means that the participants feel secure while using credit cards for their online payments

2.1.6 Frequency of Credit Card Fraudulent Issues

H0: No security issues and credit card fraud happened frequently.

H1: having security issues and credit card fraud happened frequently.

Table: 9 Frequency of cyber security issues faced by credit card users in KSA.

		Has your card been subjected to any fraud?			P-value
		I don't know	No	Yes	
Have you had any problems with breaching security/privacy?	I haven't had problems breaching security/privacy, and I'm not worried about these issues.	5 (18.51%)	74 (16.26%)	5 (6.94%)	0.000
	I haven't had problems breaching security/privacy, but I worry about these issues.	18 (66.6%)	344 (75.60%)	40 (55.5%)	
	I've recently had problems breaching security/breaching privacy, and I'm concerned about these issues.	4 (14.81%)	37 (8.13%)	27 (37.5%)	
Total		27	455	72	

In the above table no.9, we have seen that people were having the security and privacy issues and (55.5%) were already had the online transaction through the credit card faced the fraud and they are worried about the issues and problems regarding this matter the p-value is found to be significant hence we reject the null hypothesis.

2.1.7 Sharing of Personal Information with Government and other Websites

H0: People shared their personal information with-government and over websites.

H1: People doesn't share their personal information with-government and over websites.

Table: 10 Willingness to share your private information with government and other websites

		Do you realize that you share your personal information with e-government services?		Total	P-value
		No	Yes		
Have you shared your phone number or personal information online without reading the website's privacy policy?	No	44 (17.39%)	209 (82.60%)	253	0.649
	Yes	48 (15.94%)	253 (84.05%)	301	
Total		92	462	554	

We have observed in table 10 that the study participants are found to be more eager in sharing their personal information with the e-government and the other online websites (84.05%) which is also the evidence that they trapped in the fraud because of the leaking their personal information to the online websites the p-value is non-significant hence we accept the null hypothesis. People are willing to share personal information with the government.

2.1.8 Sharing of Information with Unknown Sources:

It has been observed that people may click links from some unknown sources accidently or willingly and may face cybersecurity issues. A question was asked from public participants.

Table 11: Participants interact with anonymous links

		Frequency	Percent
Have you clicked on any electronic links you have received via SMS, anonymous WhatsApp messages, email or any other anonymous media?	No	376	67.9
	Yes	178	32.1
	Total	554	100.0

In the above table we observed that 67.9% of people are not clicking over the messages and other anonymous media and 32.1 % of them still don't know the real risks of these anonymous links and its bad effects.

2.1.9 Trends in Use of E-commerce

H0: People having high interest in participating e-commerce and Saudi Arabia is shifting towards the e-commerce.

H1: People doesn't have high interest in participating e-commerce and Saudi Arabia is not shifting towards the e-commerce.

In table 12 there is a high percentage of study participants who would like to participate in the e-commerce training courses and they also think that Saudi Arabia is shifting towards the e-commerce. This means that citizens are highly interested in e-commerce, and they are also willing to participate in trainings for its better use.

		Would you like to participate in an e-commerce training course?			Total	P-value
		I don't know	No	Yes		
What is Saudi Arabia's shift towards e-commerce?	High	34 (11.52%)	62 (21.01%)	199 (67.45%)	295	0.789
	Low	1 (10%)	3 (30%)	6 (60%)	10	
	Medium	24 (16.43%)	28 (19.17%)	94 (62.32%)	146	
	Very high	10 (9.70%)	20 (19.41%)	73 (70.87$%)	103	
Total		69	113	372	554	

Table: 12. participants liking to adopt e-commerce and online training on its use

2.1.10 E-commerce Vs Traditional Trade:

Table: 13. Comparison of e-commerce and traditional trade

		Frequency	Percent
Do you think e-commerce will be a good alternative to traditional trade?	I don't know	70	12.6
	No	73	13.2
	Yes	411	74.2
	Total	554	100.0

The above table 13 shows that (74.2%) people thinks that e-commerce will be a good alternative to traditional trade which means they are not more flexible with the current trade (86.8%) study participants expects that e-commerce to have a successful future in Saudi Arabia over the next five years as shown in the below table.

2.1.11 Trends in E-Commerce Success:

Table:14. E-commerce success over a period of five years

		Frequency	Percent
Do you expect e-commerce to have a successful future in Saudi Arabia over the next five years?	I don't know	57	10.3
	No	16	2.9
	Yes	481	86.8
	Total	554	100.0

The above table shows that most of the people (86.8%) foresee the successful growth of e-commerce in Saudi Arabia. They expect its bright future in next five years.

2.2 LACK OF AWARENESS AND TRAINING DEVELOPMENTS

2.2.1 IT Specialist's Perceptions

Table: 15. Need of awareness of cyber threats

Variable	Strongly disagree	Disagree	Neutral	agree	Strongly agree
How strongly you think it is good to have every Saudi citizen to be aware of Cyber threats?	0	1 (1%)	4 (3.8%)	21 (20.2%)	77 (74%)

The table shows that 74% of the respondents are strongly agree that citizen of Saudi Arabia should be aware of cyber threats. Similarly large number of respondents believe that Saudi Arabia have potential technology to defend all the cyber related threats. These results suggest that if citizen of Saudi Arabia have potential of knowledge about cyber threats, then they would look forward to applying strong security to secure their assets.

Table 16: Participation in cyber security awareness program by IT experts

Variable	Yes	No
Have you participated in cyber-security community awareness?	42 (40%)	61 (58%)

Table.16 shows that majority of IT specialists have not participated in such awareness program if not arranged by the government i.e. 58%.

Table:17. Willingness to participate in cyber security awareness program

Variable	Yes	No
Will you be interested in promoting cyber-awareness program to community, if the government provides some incentive for you?	100 (97.09%)	3 (2.91%)

Table 17: shows that majority of IT specialists (97%) are interested to participate in cyber security awareness program if supported from the government.

Table: 18. Importance of safety of personal information

Variables	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
How strongly you agree this statement: Keeping personal and identifiable information safe and secure is at most priority.	22 (21%)	18 (17.1%)	3 (63%)	0	0

Yes, it is important to safe your personal information and do not share with anyone as 63% of the population neutral with this statement. And 21% of the population are strongly agreed.

Table: 19. participants response if they are provided with incentives on serving the community

Variable	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
How satisfied are you if we give you benefits and incentives when you serve the community?	61 (58%)	39 (37.1%)	3 (2.9%)	0	0

58% and 37.1 % of the participants are strongly agree and agree respectively with this statement that if they serve the community they will be given with benefits and incentives.

Table: 20. Participant response on getting the chance to participate in completive program.

Variable	Strongly dissatisfied	Dissatisfied	Neutral	Satisfied	Strongly satisfied
How satisfied are you if given chance in a competitive program with special privileges?	2 (1.9%)	11 (10.5%)	40 38.1%	48 (45.7%)	0

45.7% of the participants are satisfied when they get the chance to participate in competitive programs with special privileges. While 38.1% participants showed neutral behavior to participate in such programs.

2.2.2 Knowledge of Cybersecurity

H_0: The respondents do not have the knowledge of cybersecurity and basic concept of cyberattacks.

H1: The respondents have the knowledge of cybersecurity and basic concept of cyberattacks.

Table: 21 Participants' perception about their knowledge of cybersecurity.

		Do you know anything about cybersecurity?			Total	P-value
		I don't care	No	Yes		
Female	Do you think it's important to learn the basics of the concept of cyberattacks?	I don't care	11 (28.2%)	25 (64.10%)	3 (7.69%)	39	0.000
		No	4 (26.66%)	11 (73.3%)	0	15	
		Yes	6 (3.94%)	79 (51.97%)	67 (44.07%)	152	

	Total	21	115	70	206	
Male	Do you think it's important to learn the basics of the concept of cyberattacks?	I don't care	19 (43.18%)	19 (43.18%)	6 (13.63%)	44	0.000
		No	0	13 (76.47%)	4 (23.52%)	17	
		Yes	15 (5.22%)	113 (39.3%)	159 (55.40%)	287	
	Total	34	145	169	348	

In table 21 we have observed that the study participants are highly aware of the cybersecurity, and they have the basic knowledge about the cyberattacks in females the percentage is (44.07%) and in males (55.40%) which is quite a good percentage of evidence that they have the awareness of cyberattacks thus the p-value is also found to be significant, so we reject the null hypothesis.

2.2.3 Cybersecurity adoption post Fraud Experiences

H0: People who are already got online fraud are not interested in having the cybersecurity courses.

H1: People who are already got online fraud are interested in having the cybersecurity courses.

Table: 22. Fraud experiences and adoption of cybersecurity in future

		Are you interested in attending an awareness course on cybersecurity or any course on security?			Total	P-value
		I'm not interested	No	Yes		
Has your card been subjected to any fraud?	I don't know	4 (14.81%)	2(7.40%)	21 (77.7%)	27	0.056
	No	96 (21.09%)	25 (5.49%)	334 (75.60%)	455	
	Yes	6 (8.33%)	8 (11.11%)	58 (80.55%)	72	
Total		106	35	413	554	

In table 22 we have observed that the respondents had the fraud of online transaction through their credit cards are interested in attending the courses about the cybersecurity the results are insignificant hence we accept the null hypothesis.

2.2.4 Availability of Equipment

It is a matter of concern that the survey and other related awareness program can be effective if the users have proper access to IT equipment's e. g. mobile phones with 4G or 5G, IPADs, Laptops, personal computers connected with internet etc.

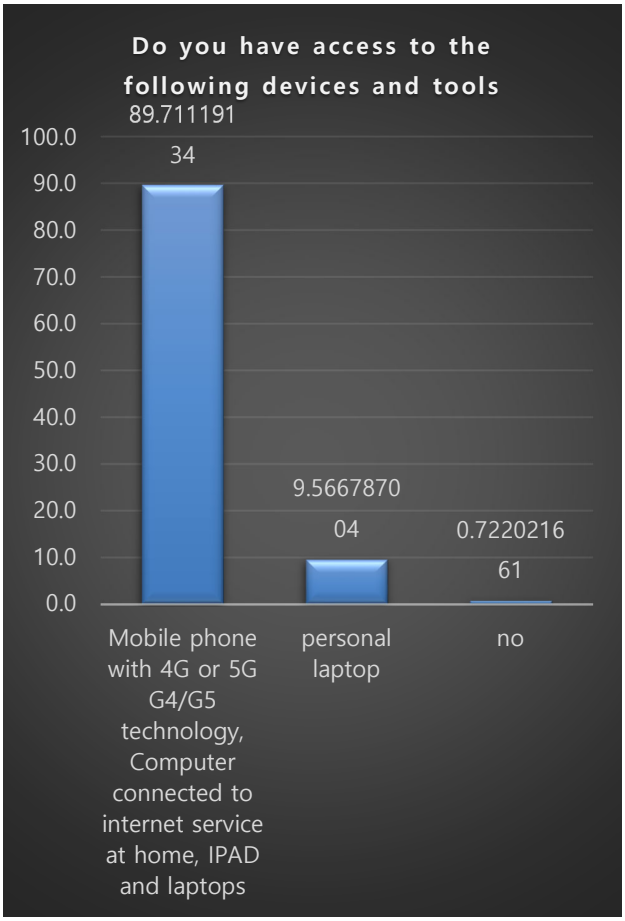

Figure 5. Using digital devices

The above graph shows that there are 89.7% participants who have the access of these digital devices which is the largest percentage among the responses.

2.2.5 Use of Technology against Small Payments

H0: People don't know the basic use of technology neither they are interested to pay fee for a small course about it.

H1: People know the basic use of technology and they are interested to pay fee for a small course about it.

Table: 23. Willingness to pay small amounts for using technology

		Do you know the basics of using technology?			Total	P-value
		I don't know	No	Yes		
Are you ready to pay a small fee for the course?	No	41 (57.74%)	45 (45%)	148 (38.64%)	234	0.009
	Yes	30 (42.25%)	55 (55%)	235 (61.35%)	320	
Total		71	100	383	554	

In table 23 we have observed that the study participants know the basic use of technology and they are also interested in paying fee for attending the course regarding this matter the p-value is significant hence we reject the null hypothesis.

2.2.6 Participation in Trainings

H0: People have already taken the technology training courses and ready to pay small fee for course.

H1: People haven't already taken the technology training courses and ready to pay small fee for course.

Table: 24 participants' interest and willingness to participate in trainings

		Have you ever participated in a technology training course?		Total	P-value
		No	Yes		
Are you ready to pay a small fee for the course?	No	159 (49.22%)	75 (37.3%)	234	0.077
	Yes	194 (54.95%)	126 (62.68%)	320	
Total		353	201	554	

In the table no.24, it clearly shows that the people having the highest percentage (62.68%) of having the technology training courses and are also eager to pay the fees for more courses. The p-value is non-significant hence we accept the null hypothesis.

2.3 IMPACTS OF CULTURE

2.3.1 Citizen feelings to the future smart cities' infrastructure

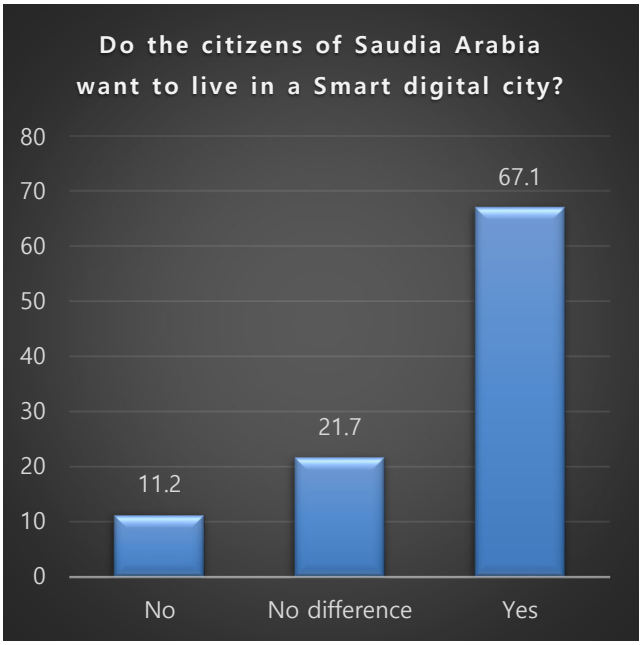

Figure 6: like to live in a smart digital city

The above graph shows that citizens (IT experts) of Saudi Arabia wants to live in a digital smart city, as 67.1% of population say yes to this question.

2.3.2 Awareness to Cyber Threats

Table: 25. Believe that Saudi Arabia is not ware of cyber threats

The above table shows that most of IT Specialists are agreed that more than 50 % of Saudi citizens are not aware of current cyber threats. People use their IT devices without taking the cyber threats into their considerations.

Variable	< 10 %	20 % - 30 %	30 % - 40 %	40 % - 50 %	>50 %
To your knowledge, what percentage of Saudi citizens are not aware of current cyber threats?	3 (2.9%)	6 (5.8%)	18 (17.3%)	25 (24.0%)	51 49.51%

2.3.4 IT infrastructure and Saudi Culture

Table: 26. Effect of IT infrastructure on Saudi culture

In table 26 maximum number of citizens (40%) are neutral with this statement as they perceive that advancement in IT infrastructure will not affect Saudi culture. However, 32.4% IT experts think that advancement in IT infrastructure will affect the Saudi culture i.e. 40%. 14.3% of the population is strongly agree with the statement that Saudi Arabia is being affected with good IT infrastructure.

Variables	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Do you believe advancement in IT infrastructure will affect the Saudi culture	15 (14.3%)	34 (32.4%)	42 (40%)	7 (6.7%)	5 (4.8%)

Table; 27. Social apps affecting Saudi culture

Variables	Twitter	Snapchat	WhatsApp	Instagram	Others
34. Provide two important Technology Apps (Social Apps) that affect Saudi culture.	34 (32.4%)	54 (51.4%)	15 (14.3%)	0	0

The above analysis shows that yes culture of Saudi Arabia is affected by these social apps. As 51.4% of the population agree with this statement. Analyzing the results, it has been observed that snapchat (51.4%) and Twitter (32.4%) are the two mostly used social media apps in the Saudi Arabia which are affecting Saudi culture

2.3.5 Awareness about Smart Cities in Saudi Arabia

H0: The respondents are not aware neither they want to live in a smart city.

H1: The respondents aware and they want to live in a smart city.

Table: 28. Saudi residents' interest to live and adopt lifestyle in smart cities

		Would you like to live in a smart digital city?			Total	P-value
		No	No difference	Yes		
Are you aware of the terms of smart cities?	No	51 (82.25%)	104 (86.6%)	252 (67.74%)	407	0.000
	Yes	11 (17.74%)	16 (13.33%)	120 (32.25%)	147	
Total		62	120	372	554	

In table 28 we have observed that the respondents are aware of the term smart cities, and they want to live in the smart cities the results are significant.

2.4 SHORTAGE OF LOCAL EXPERTISE

2.4.1 Technical ability of IT specialists

Variable	Yes	No	I don't know
Do you have the technical ability to perform network-wide deep-packet inspections?	12 (11.4%)	43 (41%)	48 (45%)

Table: 29 shows that participants do not have much ability to perform network wide deep- packet inspection, as 41% of the respondents says no to this statement while 45% respondents replied as they don't know this term.

2.3.2 Private sector Job Satisfaction

Table: 30. Participants' satisfaction in working in the private sector

Variable	Strongly dissatisfied	unsatisfied	Neutral	Satisfied	Strongly satisfied
Participant's preference in working in the private sector	2 (1.9%)	0	11 (10.5%)	37 (35.2%)	51 (48.6%)

The above table shows that majority of the IT experts (48.6%) are strongly satisfied while working in the private sector. While 35.2% expressed that they are satisfied. Overall IT experts like to work in private sector.

Table: 31. Reasons of working in the private sector

Variable	Frequency
Financial advantages (bonuses, incentives)	26 (25.24%)
Good salary	40 (38.83%)
Training programs	15 (14.56%)
Professional work environment	10 (9.70%)
Career development	15 (14.56%)

The above table shows that participants are more interested in working in the private sector as private sector provide them attractive salary package along with other incentives (bonuses, tours etc.) A reasonable percentage (15%) has shown the working in private sector as a result of good opportunities of professional trainings.

2.3.3 Public sector Job Satisfaction

Table: 32. Reasons to avoid working in the public sector.

Variable	Frequency
Improper infrastructure	15 (14.56%)
No incentives on work/ lack of development/low salaries	33 (32.03%)
Lack of trainings	30 (29.12%)
Minimum growing opportunities	25 (24.27%)

The above tables shows that IT Specialists are not much satisfied working in the public sector because of the reasons like, improper infrastructure, lack of incentives, low growth and low salaries.

Table: 33. How Can public sector meet private sector in the future in terms of facilities provided to their employees

Variable	Frequency
Financial advantages (bonuses, incentives)	20 (19.41%)
Good salary	38 (36.89%)
Training programs	12 (11.65%)
Professional and pleasant work environment	13 (12.62%)
Career development via trainings and course	20 (19.41%)

36.89% of the people believe that by providing high salaries and on providing financial benefits and career development courses public sector can meet the level of private sector in future.

2.3.4 IT specialists' Job Satisfaction

Table: 34. How Strongly IT specialists are agreeing with the statement that public sector provides job satisfaction in the new future:

Variables	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
How strongly you agree with the following statement: Public sector and governmental agencies can match private sectors in the new future:	38 (36.2%)	38 (36.2%)	20 (19%)	4 (3.8%)	3 (2.9%)

Table shows that, yes IT professionals are agree with the statement that public sector or government agencies provides job satisfaction. i.e., 36.2% for both agree and strongly agree. This means that IT professionals are looking forward to getting the jobs in government sector in the future if match the private sector.

3. Reliability Analysis of Data Collected

3.1 IT Specialists' Survey

Reliability Statistics	
Cronbach's Alpha	N of Items
.728	21

Table: 35: The Cronbach's alpha (0.728) shows that there is a sufficient consistency between the variables as the value of 0.7 or above is highly consistent.

3.2 Public people Survey Data

Reliability Statistics	
Cronbach's Alpha	N of Items
.853	14

Table: 36: According to Cronbach's alpha (0.853) the variables are highly related and consistent as the value of 0.7 or above is highly consistent.

4. Study Discussion & Result Evaluation:

In our study the total number of respondents in the public sector data was 554 in which 348 males and 206 females in the survey; and the ICT survey we had 103 total respondents in which 73 were males and 30 females. Table 2 shows that Saudi Arabia need to improve its cyber security platform. As 42.9% of the population strongly disagree with this statement. Citizen of Saudi Arabia may face threats in the form of internet scams, WhatsApp links, hack bank account, bank fraud, and social media scams. This is the clear evidence that Saudi citizens have no trust on cyber security platforms. Table 2 also shows that participants of the study does not believe that Saudi Arabia has enough knowledge and capacity to allocate smart city facilities. 33.3% participants strongly expressed their concerns about the capacity to run smart cities. They have also shown lack of knowledge of capacity to adopt and live-in smart cities. According to the results of table 3, it has been seen that yes Saudi Arabia is moving towards digital economy. i.e., 67.6% of the people are strongly agree and 23% are agree. This reflects the tendency of the people to wards digital economy. Table 5 shows that the citizens consider that improper cyber security system (30.09%) is the major parameter of lack of trust on cyber infrastructure following unprofessional work environment (27%). Table 6 demonstrates that the internet speed has the influence over the awareness of smart devices in which we come to that people having the fastest speed having the less percentage (34%) whereas the people having the medium speed having the higher percentage which is (47.29%) so it shows that the awareness or knowledge about the smart devices is not depending upon the internet speed they had it is about the matter of interest. We may elaborate that the speed of

internet and connectivity of smart devices is significantly associated with each other. In table no.8 we observed that the female respondents having less percentage of facing fraud and problems of security and privacy which is like (18.18%) however the results are found to be significant and in males the percentage is higher which (50%) of the respondents have been in the issue of fraud and they are going through the problem of security and the participants feel secure while using credit cards for their online payments. In the table 9, we have seen that people were having the security and privacy issues and (55.5%) were already had the online transaction through the credit card faced the fraud and they are worried about the issues and problems regarding this matter. We have observed in table 10 that the study participants are found to be more eager in sharing their personal information with the e-government and the other online websites (84.05%) which is also the evidence that they trapped in the fraud because of the leaking their personal information to the online websites.

In table 7 we have observed that both male and female respondent are aware of the digital economy, and they are making online transactions and online shopping etc. The percentage in female (70.21%) and in males (84.38%) which is quite a high percentage showing that they have the knowledge, and they are making online transactions whereas the p-value is found to be non-significant in females and significant in males. This means that males are aware of digital economy, and they are significantly involved in e-commerce while female are reluctant to adopt e-commerce. In table 17 there is a high percentage of study participants who would like to participate in the e-commerce training courses and they also think that Saudi Arabia is shifting towards the e-commerce. This means that citizens are highly interested in e-commerce, and they are also willing to participate in trainings for its better use. Table 13 shows that (74.2%) people thinks that e-commerce will be a good alternative to traditional trade which means they are not more flexible with the current trade (86.8%) study participants expects that e-commerce to have a successful future in Saudi Arabia over the next five years.

All the factors such as cyber infrastructure issues, services from governments or companies, cyber threats attacks, and cyber based economy limit cybersecurity frameworks adoption in Saudi Arabia are closely associated with lack of trust among the users of IT statistically, Hence, our hypothesis (H1) is strongly supported that there is a lack of trust persists among IT users regarding infrastructure etc. It has been observed that there is dire need to launch a comprehensive awareness program regarding cybersecurity and related frameworks so that the trust level of the users may be enhanced towards a digital economy in KSA.

The table 15 shows that 77% of the respondents are strongly agree that citizen of Saudi Arabia should be aware of cyber threats. Similarly large number of respondents believe that Saudi Arabia have potential technology to defend all the cyber related threats. These results suggest that if citizen of Saudi Arabia have potential of knowledge about cyber threats, then they would look forward to applying strong security to secure their assets. Majority of IT specialists have not participated in such awareness program if not arranged by the government. While majority of IT specialists (97%) are interested to participate in cyber security awareness program if supported from the government.

58% and 37.1 % of the participants are strongly agree and agree respectively with this statement that if they serve the community they will be given with benefits and incentives. 45.7% of the participants are satisfied when they get the chance to participate in competitive programs with special privileges. While 38.1% participants showed neutral behavior to participate in such programs (Table 20). In table 21 we have observed that the study participants are highly aware of the cybersecurity, and they have the basic knowledge about the cyberattacks in females the percentage

is (44.07%) and in males (55.40%) which is quite a good percentage of evidence that they have the awareness of cyberattacks. In table 9 we have observed that the respondents had the fraud of online transaction through their credit cards are interested in attending the courses about the cybersecurity. In table 23 we have observed that the study participants know the basic use of technology and they are also interested in paying fee for attending the course regarding this matter. In the table 24 it clearly shows that the people having the highest percentage (62.68%) of having the technology training courses and are also eager to pay the fees for more courses.

All the above results validate our hypothesis (H2) that there is a need to have cyber security awareness programs to develop a trust level based on trained personnel who may play their role to build that required trust.

Table 25 shows that most of IT Specialists are agreed that more than 50 % of Saudi citizens are not aware of current cyber threats. People use their IT devices without taking the cyber threats into their considerations.st level and awareness among IT users. In table 26 maximum number of citizens (40%) are neutral with this statement as they perceive that advancement in IT infrastructure will not affect Saudi culture. However, 32.4% IT experts think that advancement in IT infrastructure will affect the Saudi culture i.e. 40%. 14.3% of the population is strongly agree with the statement that Saudi Arabia is being affected with good IT infrastructure. The analysis shows that yes culture of Saudi Arabia is affected by these social apps. As 51.4% of the population agree with this statement. Analyzing the results, it has been observed that snapchat (51.4%) and Twitter (32.4%) are the two mostly used social media apps in the Saudi Arabia which are affecting Saudi culture. The statistical analysis supports our hypothesis (H3) that cultural influences, infrastructure, including a shortage of local expertise and use of social apps, awareness about cyber security influence Saudi Arabia's adoption of cybersecurity awareness methods and it is need of the hour to have a comprehensive cyber security awareness program.

Table 29 shows that participants do not have much ability to perform network wide deep- packet inspection, as 41% of the respondents says no to this statement while 45% respondents replied as they don't know this term. Table 30 shows that majority of the IT experts (48.6%) are strongly satisfied while working in the private sector. While 35.2% expressed that they are satisfied. Overall IT experts like to work in private sector. That participants are more interested in working in the private sector as private sector provide them attractive salary package along with other incentives (bonuses, tours etc.) A reasonable percentage (15%) has shown the working in private sector because of good opportunities of professional trainings. IT Specialists are not much satisfied working in the public sector because of the reasons like, improper infrastructure, lack of incentives, low growth, and low salaries. 36.89% of the people believe that by providing high salaries and on providing financial benefits and career development courses public sector can meet the level of private sector in future. IT professionals are agreed with the statement that public sector or government agencies provides job satisfaction. i.e., 36.2% for both agree and strongly agree. This means that IT professionals are looking forward to getting the jobs in government sector in the future if match the private sector (Table 34).

The above results support our hypothesis (H4) that the lack of IT professionals in public sector limits the implementation of cybersecurity frameworks in Saudi Arabia. If the IT professionals working in private sector are given proper incentives, they may play their proper role for cyber security awareness once they switch their jobs from private to public sector.

5. Conclusions:

5.1 Public People survey

Cybersecurity was well-known in the community, and residents had a basic grasp and awareness of intrusions. Members in the community have been victims of fraud and are concerned about cyberattacks. They are aware of the digital economy and engage in online transactions. Smart device awareness or knowledge is not dependent on the internet speed they have, but rather on the subject of interest. We can see that people are concerned about security and privacy, and that they have experienced online credit card fraud and are concerned about the challenges and problems that come with it. Members of the community are aware of the basics of technology and are prepared to pay a fee to take a class on the issue. A huge majority of survey respondents want to take e-commerce training courses, and they feel Saudi Arabia is moving toward e-commerce. They are also interested in technology training courses, and they are willing to pay for future courses. They feel that when the digital system is implemented in Saudi Arabia, the information technology industry will see the most growth, and that technical developments make life easier. The participants are using their credit cards frequently and from greater than 10 years. They are using the internet services frequently and they are not clicking over every massage or other link on the internet as they are careful about their personal data, the people of Saudi Arabia are highly satisfied with the e-government services they think that e-commerce will be the good alternative to traditional trade, and they also think that e-commerce will have a successful future in Saudi Arabia in upcoming years.

5.2 IT Professionals Survey

The study was carried out among Saudi Arabia Citizens as well as ICT professionals were also involved in this study, among them 73 are male and 30 are female, the research wants to investigate the digital e-commerce trend in Saudi Arabia and want to analyse whether the citizen of Saudi Arabia was aware of cyber-crime or its security measure. By applying the statistical techniques, it has been seen that people of Saudi Arabia are aware of current cyber security and they also have knowledge about cyber threats, similarly they know that advance technology can help to prevent from cyber threats or crime. Its mean that IT professional of Saudi Arabia should be potential competency to deal this issue as well as they should get special trainings so they can provide cyber security to the citizens of Saudi Arabia. Similarly, government of Saudi Arabia also play an important role to promote their IT agencies and make them better. Results suggests that Saudi Arabia is in favour of digital economy. Twitter and snapchat are two most common social media apps that widely use in the country. Results of the data also analyse that yes social media apps affect the culture of Saudi Arabia. Participants believe that cyber security system need some more improvement in the country.as 42.2% of the participants disagree with current cyber security platform, they also believe that they do not have potential technical facility to assess in this matter. ICT participants believe that it is important to secure and keep your personal identity data secure and confidential. The results obtained from ICT data set state that people have lack of knowledge and information about smart cities. Participants also believe that cyber security should practice on large scale.

It has been seen that citizen of Saudi Arabia are more satisfied in getting their jobs in the private sector as compared to the government sector because of the reason that government sector does not give higher salaries, lack of training programs, lack of career development, and low-chance of promotion. However, if government made improvements in all these factors, then government sector can be able to meet the level of private sector in future.

6. Future work

Recommendations and limitations:

To begin, future research may use more qualitative data collection methods. Because the research's subject matter is subjective and strongly relies on the opinions of individual participants, acquiring qualitative data to augment the findings given in this study might be valuable. Having participants offer more detailed comments and explain why they feel a certain way about a topic might help to strengthen the validity of the findings revealed in this study. In the future, the sample approach may be changed in addition to using more qualitative sampling techniques. Results from random sampling approaches may be generalizable to the full population. Another exciting aspect would be to include clients of all ages. Because this study focused solely on adults, the results cannot be applied to other age groups. Other characteristics, such as age, different profession, and education, should be explored as well to see whether they have any cybersecurity issues. While the questionnaire provides important feedback regarding critical study issues, it fails to offer the researcher the opportunity to clarify issues. It is necessary that all elements of the questionnaire, from design to choosing the suitable target-group, are considered, to gather the maximum amount of reliable and valuable information. The result of the analysis shows that advance techniques in IT infrastructure may affect the culture of Saudi Arabia. Therefore, they should develop effective IT strategies as well as cyber security policies in order to secure their nation from cyber threats.

7. References

[1] Chigbu, Uchendu E. “Visually hypothesising in scientific paper writing: Confirming and refuting qualitative research hypotheses using diagrams”. *Publications*, vol. 7, no. 22, 2019, pp. 1-18.

[2] Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. NursingPlus open, 2, 8-14.

[3] Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. Administration and Policy in Mental Health and Mental Health Services Research, 42(5), 533-544. https://doi.org/10.1007/s10488-013-0528-y

[4] Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. Journal of applied management accounting research, 10(1), 69-80.

Dr. Prakash Veeraraghavan
Assoc Prof, Comp Sci and IT, Computer Science & Information Technology

Nawaf Alhalafi PhD Student at La Trobe University, Computer Science & Information Technology Department.