Differences in Users' Insights and Increase in The Acceptance Level for Using The BYOD Approach in Government, Non-Profit Organizations, and Private Sectors in Saudi Arabia

Ahmed M. Alghamdi [1*], Adel A. Bahaddad [2], and Khalid A. Almarhabi [3]

[1] Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 21493, Saudi Arabia

[2] Department of Information System, Faculty of Computing and Information Technology, King Abdulaziz University Jeddah 21589, Saudi Arabia

[3] Department of Computer Science, College of Computing in Al-Qunfudah, Umm Al-Qura University, Makkah 24381, Saudi Arabia

*Corresponding author: Ahmed M. Alghamdi; *amalghamdi@uj.edu.sa*

Summary

Digital transformation represents one of the main obstacles facing several government, private, and non-profit sectors that help stabilize digital transformation in the Arabic region. One of the helpful ways to improve the level of freedom, productivity, and flexibility among employees to accept the BYOD approach is using their own devices to perform their work both in and outside the workplace. This study focuses to present the differences between the main three economic sectors, which represent the most important pillars of the economy in Saudi Arabia within the Kingdom's Vision 2030. BYOD also has great importance to the stakeholders for raising their awareness by expressing the implications, if the concept of BYOD is widely and correctly adopted. The study uses the diffusion of innovation (DOI) framework and quantitative analysis data to determine the main dimensions and important factors that help increase the awareness of the target audience. The number of participants in this study was 830, and the participants are mixing between the government, private, and non-profit sectors. The main findings showed a significant impact of several factors such as the importance of knowledge, ease of use, employee satisfaction, risk awareness, and attention to increase the level of acceptance in three main sectors study for using the BYOD approach widespread and professional use.

Keywords:
Bring Your Own Device (BYOD), Diffusion of Innovation, Saudi Arabia, COVID-19, Comparative Study

1. Introduction

Many countries around the world are seeking to take advantage of digital transformation for enhancing their strategic goals and services [1]. Therefore, governments are looking to invest and take advantage of digital transformation between governments and both the public and private sectors for changing economic needs and activating digital technologies for providing products that help to facilitate work and manage human resources professionally [2]. Consequently, digital transformation seeks to develop users' thinking about benefiting from business models in line with continuous technical developments, raising operational efficiency, and reducing the rate of errors and defective aspects in the provided services [3]. Additionally, countries seek to take advantage of the great chance of the fourth economic revolution to create a digital economy that depends mainly on providing and expanding technological opportunities to enhance customer and employee satisfaction, increased revenue, and innovation inspiration [3]. From this standpoint, the KSA, represented by its 2030 vision, is seeking to reach one of the top ten places in the Global Competitiveness Index, as it surpassed 15 places between 2017 and 2020 according to the Global Competitiveness Index of the Institute for Administrative Development (IMD). This proves that progress in overcoming all the difficulties facing this transformation is being made through the potential of the fourth economic revolution [3, 4]. After the widespread COVID-19 pandemic, digital economy trends have taken advantage of technology by using the data and digital content artificially to automate the processes of cooperation between government agencies and private companies [5]. As a result, governmental organizations and the private sector have reached an advanced level by understanding the importance of using technology for facilitating digital transformation [6]. It helps with the continuation of social and economic activities despite closures and social distancing in many communities. During the last years in 2020, the KSA was keen through the global pandemic to provide the capabilities and enablers to accelerate the process of digital transformation through a package of government aids such as providing cloud storage, providing a governance framework for most government transactions, and providing the infrastructure that ministries and institutions need to reach the beneficiaries technically [6, 7]. Furthermore, the government provides an integrated field of various data banks and links them with each other to

provide the possibility of serving beneficiaries more professionally and ensuring the provision of acceptable and satisfactory digital services to communities and individuals [7]. In the following points, the research paper covers the BYOD definition, the main challenging aspects of adopting the BYOD in different sectors, an overview of the public, private, and non-profit sectors, presenting previous studies that focus on the context of the study scope, methodology of data analysis, and discussing of preliminary results and their implications for the research.

1.1 BYOD Definition

Many of the various ways that help increase rates of digital transformation at the individual, governmental, and private sector levels fall under the Bring Your Own Device (BYOD) approach. This approach focuses on employees using their personal devices to connect to their organization's network and systems. BYOD is making great progress in the business world, with around 75% of employees in high-growth markets like Brazil and Russia and 44% in developed markets already using their personal devices at work [8, 9]. The literature indicates that companies are unable to prevent employees from bringing personal devices into the workplace, and thus their personal devices can be utilized in various aspects of work. One study showed that around 95% of employees stated that they use at least one personal device at work, which is one of the various benefits of the expansion of work in the context of the BYOD approach [9, 10]. Some of the added benefits are reduced expenses and service agreements, as they help enhance employee mobility, productivity, satisfaction, and flexibility. BYOD helps share information and communications in real-time and can be accessed from anywhere, even without a LAN or Wi-Fi network available [9, 11]. Therefore, this study seeks to discover the basic and necessary awareness of employees in different sectors as to how to activate the BYOD approach to raise efficiency and rationalize spending more professionally.

BYOD includes personal devices such as laptops, tablets, and smartphones that employees are allowed to use to carry out business functions [9]. The high expenses of information technology make this challenging in critical sectors, including the public and private sectors [9]. Moreover, It is difficult to sustain the life cycle of technical hardware, especially when the economy is affected by commercial movement, as in the coronavirus pandemic [10]. Thus, providing this service to the public takes priority over back-office support to keep things running. Financial movement and budgets affected by the high economic recession will remain negative for a while and will not change soon [9, 12]; therefore, BYOD policy helps to fulfill some requirements of running an office business in light of the scarcity of occupying various physical office workspaces. I could bring my own device and use it for my

work to save the usual life cycle cost [12]. However, how do we overcome the many issues that arise as a result of using the BYOD approach? One example of these issues is awareness of the importance of the BYOD concept in terms of security. This covers several main issues that are important to focus on to raise BYOD awareness in the public, private, and non-profit sectors [13].

1.2 Data Security

There are high risks when using the BYOD approach, especially in the public sector. The files and user information are confidential and should be protected with a high level of care. According to our previous study, most tasks carried out by normal users include completion of transactions, follow-up e-mail, and use of internal electronic systems to track the work and performance of employees [14]. Additionally, some personal information that comes from PCs or personal laptops contains data that may put the organization at risk [12, 15]. How can a public sector organization ensure an acceptable level of information security with adequate flexibility for employees using their devices and systems' services? Furthermore, cloud services such as commercial cloud and governmental cloud are another challenge because there are legitimate business reasons for accessing cloud services in both public and private sectors to avoid paying high costs for purchasing advanced maintenance and business continuity plans [9 – 11]. However, in return for these services, a vast amount of data and information can be shared with various systems through BYOD [15]. What information is collected from users? Will employee information be sold to any third party?

1.3 BYOD Policies

The policies for BYOD are an integral part of the governance that many government agencies and private companies are looking to provide and activate for desktops, laptops, personal tablets, smartphones, and other devices for business purposes [12]. Therefore, the BYOD policy is part the of risk management policy and security issues policy that is associated with company files accessed with personal devices [15]. Thus, organizations may decide to develop a BYOD policy to meet the needs of their employees or for other business reasons, or providing complementarity between information technology policies in organizations [15].

BYOD has been widely adopted by the private sector, with an estimated 74% of companies using or planning its adoption in the not-too-distant future, but the public sector doesn't seem to share this enthusiasm [17]. Also, recent statistics indicate that up to half of the councils in London do not have a BYOD policy in place [16]. Additionally, there are many government attempts to regulate BYOD in the governmental and private sectors to determine the level

of authority at which employees are permitted to access data and applications using their own devices. An example is the Canada Education Savings Grant (CESG), which is the information security arm of the Government Communications Headquarters (GCHQ) and its British state affiliates. Many public parties such as local councils seek to introduce the BYOD approach to provide more flexible work for employees [14]. CESG details the security rules that must be followed for any mobile device, but it allows for the first time the use of employee-owned computers [18].

The policies can be distributed according to their main classification security parts. Some examples of these policies are that any mobile device must be returned to a factory setting before it is used to access government data, that the device must be able to be fully managed by the organization used throughout its use for mobile work, and the organization can also ensure that information security policy is applied in the device's enterprise management [17, 18]. Furthermore, CESG has recommended 12 legislative articles to control and secure data in transit and certify safe embarkation, including detection and prevention of malicious code and an accident response plan for security issues such as hardware loss [14]. Additionally, using the device with a BYOD approach should be supported by specific approved and implemented electronic security standards, employee agreements, and cybersecurity awareness training. Moreover, connecting to public Wi-Fi hotspots and avoiding malware are other security concerns when discussing BYOD [14, 15]. Thus, some regulations should be added to data production policies such as the General Data Protection Regulation (GDPR), which adds more policies to production data laws, and a higher level of protection will have to be provided for sensitive personal data, which may create a potential bog for IT departments as they seek to incorporate BYOD into their plans [15].

1.4 Permissions and Authorizations

Determining who is allowed to use and transmit access to potentially highly sensitive information is not a simple task [5]. Therefore, informing the employees what they are and are not allowed to do on their devices without restricting these powers may lead to more confusion [12]. Thus, one cause of concern for many governmental and private organizations is the use of different devices and how IT professionals ensure a common experience across all areas while ensuring no leaks or breaches. The similarities in the hardware and software can be expensive, but it comes with the peace of mind that's conspicuously absent when BYOD is in action [19].

1.5 BYOD Benefit

There are some benefits to using the BYOD approach that can be summarized in the following points:

- BYOD has the power to rationalize spending, but this should be carefully weighed against the risks. BYOD has moved from a $67 billion industry to a $181 billion industry by the end of 2020, something that will become increasingly difficult to ignore in the future [14, 15].
- Employees enjoy greater freedom and flexibility to use their own devices to do their jobs [9, 11]. Also, employees enjoy and feel comfortable using their own devices, which they believe leads to higher productivity.
- The end-user devices are owned by the companies or managed by IT departments in government institutions under agreements that provide employees with a selected set of devices [12, 15]. In this way, users have a choice between the number of devices that are fully supported while the enterprise benefits from enhanced security features and common productivity standards found in business devices such as ThinkPad and ThinkCentre.
- It can have priority access to technical support and services contracted within the BYOD service, thus maintaining the highest standards of security, support, and improved software commensurate with the spread of BYOD [14].
- Using Windows 10 Pro's security features designed for BYOD encrypts all data on the device in case of unauthorized access [20].
- Auditing roles within the organization helps to identify many aspects with different features and roles that have their own advantages. Such devices are equipped with Intel® Active Management Technology, which enables IT managers to discover, repair, and help protect networked computing assets [19]. They can also remotely erase all data on a lost or stolen device

1.6 The Main Three Labor Sectors Working In KSA

Three main sectors have been largely activated in the Kingdom's Vision 2030 due to their great contributions to serving society and building the Saudi economy [21]. These sectors can be utilized in building and activating various qualitative initiatives that greatly increase the level of productivity. These sectors are the public, private, and non-profit sectors. Below is an explanation of each sector in more detail.

- The public sector or the government sector: The public sector in KSA is known as the government sector and the public sector. This acronym is used to signify all economic activities of government agencies. These activities are based on governmental ownership of products, capital, and services [21, 22]. The public sector provides many services that may operate in the interests of the Saudi people. This sector is not limited

to a specific category of people and communities, unlike the private sector [23]. Both the public and private sectors follow one criterion, which is the legal form of ownership. The KSA has recently witnessed an expansion in public sector activities to include all public government interests such as security, defense, judiciary, education, and health, which are subject to supervisory standards and financial regulations followed by the government, with expenditures are financed from the state budget [22, 23]. Moreover, the public sector includes public institutions, which are one main commercial domain in the public sector. This part focuses on managing some economic, social, and cultural activities according to standards of efficiency and effectiveness of performance, which are managed in a commercial manner [23]. Public institutions include public economic, investment, financing, educational, and advisory institutions, as they are distinguished by their effective roles in managing activities with a legal character independent of the state, with their own independent budgets with oversight to which the various state institutions, ministers, or governmental organizations [23, 24]. Associated with public institutions are government companies that have specific tasks of managing economic activities that are subject to full state ownership or part of its capital [23]. It is characterized by flexibility and administrative freedom from red tape, similar to private sector companies such as Saudi Aramco, Saudi Basic Industries Corporation (SABIC), Saudi Mining Company (Maaden), Saudi Unified Electricity Company, and Saudi Telecom Company (STC).

- The private sector: it is the business sector associated with companies that are personally owned by individuals and are not linked to the state's government or any of its institutions. The private sector contributes to providing empowerment and income to individuals. It is the second party and the balancing element in affecting the economic sector in every country after the public sector [23]. The private sector is considered a free field to devise profit-making strategies according to decisions appropriate to the work environment. The fields of private-sector workers are divided into individual work, which is the group of work that individuals carry out themselves without the help of other people, such as handicraft and industrial industries [14, 23]. The second part, group work, is one of the most prevalent fields of private work. It depends on the presence of more than one person in charge of the facility and its capital and has more than one employee [14, 23]. The private sector strengthens the role of private companies and raises their impact on the state's economy [21 - 23]. Examples of private sector companies include banks,

telecommunications companies, insurance companies, mobile companies, and others.

- The non-profit sector: This represents non-profit organizations and includes charitable, cooperative, and voluntary societies [25]. It can also include endowment institutions, which are established to provide all forms of cultural, religious, educational, professional, and public services without any profit motive in exchange for these services [23]. The funds of non-profit organizations are provided by the members participating in the same association or through donations or material gifts, and these funds are not refundable to their owners [25]. Non-profits can make commercial investments that benefit the organizations to ensure the survival of the organization, as well as having the advantage of being exempt from taxes. These organizations are considered credible as they are not biased towards a specific race or group and try to help everyone and find durable solutions [23 – 25]. Several studies show that the non-profit sector faces a major challenge in searching for financial stability by moving from relying on donations to relying on commercial revenue [25]. However, the modernity of this sector in many countries of the world in general, and in Saudi Arabia in particular, makes this sector dependent on donations from wealthy members of society, who have a significant influence on the way decisions are made within non-profit organizations.

1.7 Similarities and Differences Among The Three Sectors

There are many similarities and differences among the previous three sectors. The similarities can be summarized in that they all have competence in specific services that would be provided to the public in general [26]. In addition, all of them have many laws, policies, and governance frameworks that are relied upon to determine their responsibilities and jurisdictions [23 -25].

For the differences, the public sector focuses on providing services and meeting the country's citizens' needs, and the government should pay the expenses of these services to citizens in return for the taxes that the public sector collects from citizens. In the private sector, the motive behind its existence is making profits [23, 27]. Another difference between the public and private sectors is that the private sector is based on quality and encourages talent, and it has fewer regulations than the public sector, and. The public sector is rife with problems such as a lack of attention to special needs and talents, as well as gender segregation at work [23, 28]. Job security represents another difference between the private and public sectors. The public sector grants protections to its employees, as such jobs can be considered almost guaranteed. In the private

sector, however, jobs are not guaranteed, and employees can be removed even if they've held a job for years [23, 29]. Furthermore, in terms of transparency in the private sector, the level of administrative and financial corruption decreases and productivity increases based on excellence, and the level of accountability for mistakes increases, unlike in the public sector, in which productivity decreases due to its monotony [23, 28]. Additionally, there are some other differences, the most important of which is the centralized and bureaucratic structure in the public sector, while the private sector is characterized by decentralization and innovation. The public sector also aims to provide service to all citizens, while the private sector focuses on providing service to specific groups with specific needs [23, 29].

In terms of the relationship of the public and private sectors to the non-profit sector, the non-profit sector has many of the same advantages as the public sector in providing services to all citizens and providing these services depending on many policy regulations taken from the public and private sectors [23, 25, 29]. Furthermore, the non-profit sector is based on benefiting from the flexibility of the private sector in providing necessary support for its various programs through various means such as government support, donations, gifts, and investment activities [25, 29]. Additionally, the level of transparency is high in the non-profit sector, as its level of financial control increases due to the sensitivity of the funds entering the non-profit sector and its miscellaneous expenses [25, 28, 30]. Finally, the non-profit sector benefits from the creativity, flexibility, and quality of operations in the private sector, which has made the government in Saudi Arabia pay great attention to it through many diverse initiatives that should help in the advancement of the non-profit sector significantly in the future [23, 25, 28, 29].

1.8 The Kingdom's Vision of Digital Transformation

Digital transformation is one of the main aspects of the Kingdom's Vision 2030, representing a fundamental element in several ministry programs and initiatives [5, 30]. This comes from the government agencies' keenness to provide sufficient and transparent information that helps push the wheel of development economics and achieve success in various fields for government agencies [30]. Examples of digital transformation are spread across various agencies (Ministries of Health, Labor and Social Development, Justice, Interior, Education, Trade, etc.). It comes according to a general initiative focusing on launching training programs for fresh graduates to acquire fundamental and advanced skills in the modern digital technology sector to qualify job seekers and state employees to keep pace with comprehensive digital transformation [30, 31]. It is aimed at spreading digital awareness and knowledge and supporting highly qualified national cadres to push the process of digital transformation.

This initiative focuses on creating information and digital space to take advantage of the full potential of digital transformation in various agencies, institutions, and ministries [30]. Additionally, it activates the capabilities of the private and non-profit sectors to benefit from digital transformation experiences to be applied in the public sector [31, 32].

1.9 Challenges Facing the Non-Profit Sector in the Digital Transformation Field in KSA

The Kingdom's government seeks social empowerment by developing the non-profit sector by developing empowerment programs, improving their effectiveness, and qualifying the capabilities of their workers through programs that enable targeted segments to become self-reliant [30, 31]. Furthermore, it focuses on the culture of volunteer work, improving its effectiveness, and increasing volunteer opportunities by adopting the latest international methods and best practices in support of volunteering and empowering the non-profit sector [31]. Also, the KSA government is pushing to enact enabling legislation for the non-profit sector and expand the scope of non-profit organizations' services [31]. The dimension of the non-profit sector in the Kingdom's Vision 2030 looks to maximize the impact and benefits of volunteering by raising the efficiency of the non-profit sector, qualifying its workers, and enhancing their capabilities [25, 31]. Also, it aims to raise the level of local companies' contribution to supporting the non-profit sector and enhancing social responsibility in the business sector [31]. One of the most prominent challenges facing the non-profit sector in digital transformation and sustainability is the BYOD approach [28, 29, 31]. This sector needs the sustainability of the technical systems in social services, as well as improving the social services provided and increasing the effectiveness of their automation [31]. Additionally, it needs the benefits from limited collaboration and few participants by providing job opportunities and volunteer work, which helps to increase productivity and reduce the gap in volunteer work and its relevant entities' needs [31]. Throughout these challenges, the importance of the contribution of the non-profit sector to activate the role of community participation, which is one of the main pillars of the Kingdom's vision 2030 in digital transformation, and supporting it by all possible means and methods, which represent one of the main contributions of the local economy through digital transformation, is one of these means [25, 31]. Consequently, the government's initiatives support raising the level of knowledge that enables diligent and volunteer work more professionally through an initiative to automate the services and programs of associations and institutions, including technical connectivity (Nama System). This initiative aims to automate the services provided to non-profit sector

organizations and integrate their technical systems with those of ministries and other stakeholders [33].

The fundamental scope of this research is knowledge of the factors that help spread the BYOD approach in the public, private, and non-profit sectors, which will help reduce financial waste and increase spending efficiency of many diverse resources after the global recession due to the pandemic [10, 25, 26]. Additionally, it is important to determine the expected impacts on each sector if the BYOD approach is adopted, and whether these effects will impact the policies or security and data levels, as well as various usage policies [24 - 26]. The factors in the literature that increase awareness and acceptance can be divided into ten main items:

1. Knowledge, which means people know about BYOD.
2. Practice and usability, which means that people use BYOD in daily life to do their jobs.
3. Business tasks, which means the number of business tasks for which these BYOD are used.
4. Employee satisfaction, which means the number of people who feel satisfied with BYOD to do their job.
5. Risk awareness, which means the number of people aware of the risk of BYOD to employees.
6. Interest, which means the interest of users in using BYOD instead of companies providing PC devices to them.
7. Adoption, which means the final decision of users to continue adopting BYOD.

2. Related Work

Bring Your Own Device (BYOD) has been used widely for different purposes worldwide and is still growing, which makes it one of the strongest technological trends in recent years. BYOD describes the action of employees bringing their own devices to their workplaces and using those devices to complete their tasks and access the organization's information and applications [34]. The majority of research in BYOD has been related to security challenges in BYOD [5, 15, 35, 37-41], which can be classified into four categories including deployment, technical, policy and regulation, and human aspect challenges, as shown in Fig. 1.

Also, access control issues and risks for BYOD implementation have been addressed in several studies including [9, 43, 44] that introduce a new security framework using new and integrated techniques to implement access control policies in the cloud and BYOD environment. This solution is derived from considerable research into information privacy and security to manage and control access to enterprise networks by BYODs. This research has been achieved via loosely coupled integration of Mandatory Access Control (MAC) and Discretionary Access Control (DAC) mechanisms in the BYOD environment.

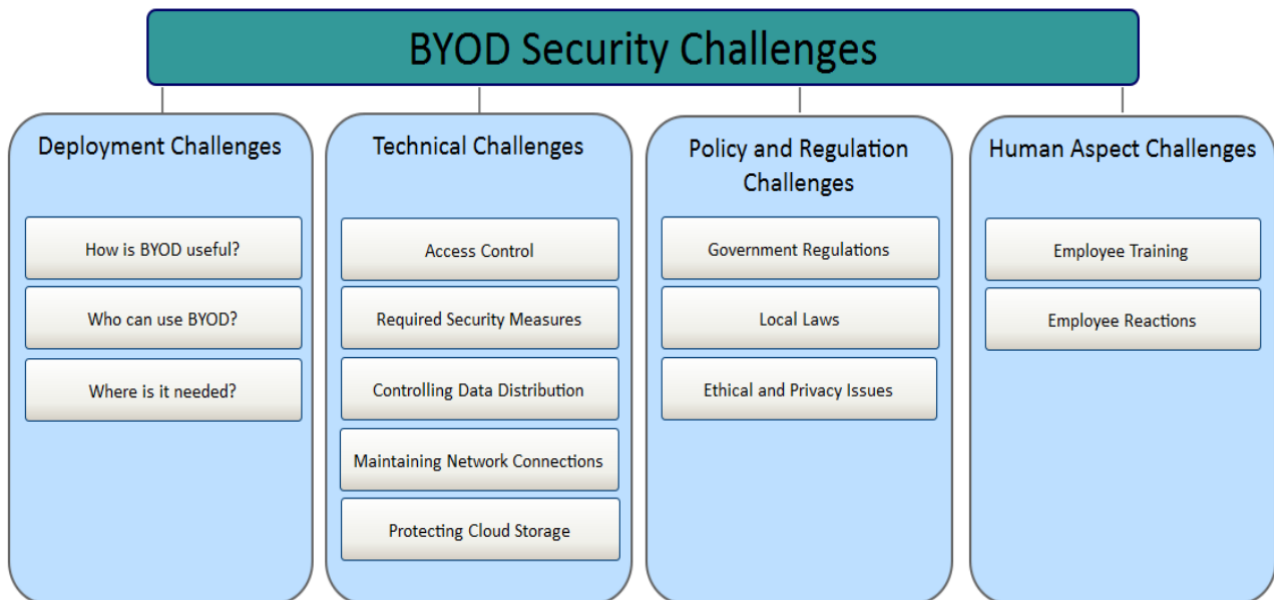In terms of the level of acceptance for using BYOD, few

Fig. 1. BYOD security challenges [8]

8. Policies and legislation, which means existing policies and legislation from the perspective of a consumer of BYOD.

studies are evaluating the use of BYOD in several nations, including the paper published in [45], to evaluate mobile device usage in higher education institutions in South Africa. However, even this paper evaluates the usage of

BYOD from a security perspective. Also, the study examined some key factors for enabling the use of BYOD in Malaysian schools for learning purposes [46, 47], which also addresses security concerns as well as identifies key factors in implementing BYOD in Malaysian schools successfully. Also, with the Malaysian aim toward BYOD implementation, some factors and proposed models have been identified and discussed for implementing BYOD in Malaysian schools [48]. The paper published in [49] assessed the control of BYOD and their secure usage in Namibian institutions of higher learning, which included case studies carried out at two Namibian tertiary institutions. Another paper investigated the level of user acceptance in using BYOD to support Hong Kong universities [50]. We noticed that many studies focus on the education sector that uses BYOD in their organizations, but some studies focus on other sectors such as a study on the banking sector in Zimbabwe published in [51], which showed how Zimbabwean banks can reduce information security risks caused by administrators using their devices in their workplaces. Finally, the employees' adoption of BYOD has been studied by integrating multi-faceted information security-related conflicts and multi-dimensional information security fatigue [52].

Regarding data security and privacy in Saudi Arabia, the paper published in [53] has investigated mobile phone security, which indicated that users in Saudi Arabia need advanced methods to protect the data stored in their mobile devices. Also, WhatsApp users' perceptions of privacy have been investigated in [54]. However, to the best of our knowledge, the situation of BYOD in Saudi Arabia has not been covered before, which needs further investigation with current developments in workplaces, especially with the current pandemic that affects interactions between users and their organizations.

3. Research Methodology

The methodology incorporated in this study for carrying out different research-related activities and collection of information on the concerned study and analysis of same has been discussed in this section of the paper. The justifications for the selection of these components of research methodology have also been provided in this section. The study has incorporated a quantitative method for assessing the aspects of BYOD and its implementation in Saudi Arabia, along with a discussion of terminology and usage. The study has incorporated this approach to determine and interpret the opinions and perceptions of the study participants in the form of comprehensive tables and charts.

The study has relied on primary data obtained from 857 participants, including 184 participants with knowledge about the concepts of BYOD. The participants included

employees working in private and public sectors as well as in non-profit organizations. Data regarding the study objectives to develop insights about the variables affecting knowledge and usage of BYOD in Saudi Arabia, as well as the distinctions among employees in different sectors, has been collected from these participants.

A structured questionnaire with closed-ended questions has been used to conduct surveys with the selected respondents. A five-point Likert scale has been used for the collection of perceptions of the participants. The questionnaire had three main components: the demographic information of the respondents, their use of personal devices at work, and their perceptions regarding BYOD.

- **Demographic information**- Gender, age, employment status, education, devices provided by the companies, and personal devices.
- **Behavior**- Usage of personal devices in workplaces and behaviors in completing jobs outside their workplaces.
- **Concept of BYOD**- Emphasis on participants with prior information about BYOD.

4. Data Analysis

The questionnaire included 29 items and its primary attributes have been discussed in this section, considering time and space constraints. Out of the sample size of 857 people, 184 (21.47%) knew BYOD, and 79.46% of the sample used personal devices for work-related matters.

4.1 Educational Qualifications of the Sample Participants

As evident from Fig. 2, the majority (46.44%) held bachelor's degrees, while 25.79% held master's degrees. The majority (85.65%) worked in different sectors. While 79.46% operate in the public sector, another 15.29% have been in private sector businesses. A small section of the participants (only 4.20%) works in non-profit organizations. The majority (46.09%) of the study respondents belonged to the 36-45-year age bracket. The female participants account for a substantially small share of the total sample (13.07%).

4.2 Knowledge of BYOD and Usage of Devices

Although females constitute a very small part of the study sample, the percentages in terms of BYOD-related knowledge are considerably similar (21.71% among males and 23.42% among females). A majority (78.53%) of the total sample size had no prior knowledge of the concerned concept, although 79.46% used devices for work purposes. This in turn highlights the threat of security issues due to a lack of knowledge of BYOD. Among the 48.66% of people

bringing their personal devices to their workplaces, only 12.37% knew about BYOD Fig. 3. shows the gender-wise participant knowledge regarding BYOD.

There is a general lack of knowledge regarding BYOD usage and its implications among general employees, and this indicates the need for organizations to incorporate awareness generation and education for users in this domain and the implications of the same.
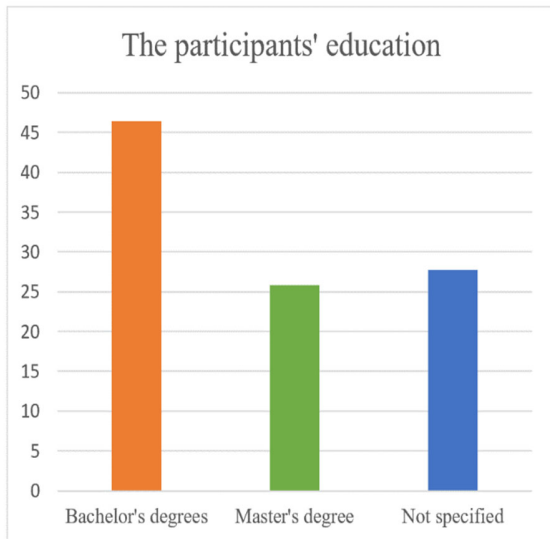

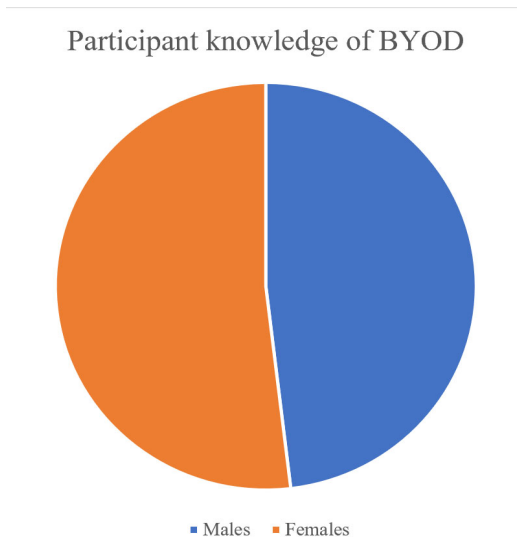
Fig. 2. Educational Qualifications of Survey Participants

Fig. 3. Gender-wise participant knowledge regarding BYOD

5. Results

The information collected in terms of the level of agreement and disagreement of employees has been analyzed, and descriptive statistics like mean, mode, and standard deviation for each dimension or factor related to BYOD and its use and perceptions have been derived and presented in Table 1 and Fig. 4.

As evident in the table, information about the perceptions and extent of relevance of aspects of BYOD among the survey participants have been collected using suitable structured questions where the answer options had been provided using a five-point Likert scale.

As evident in the table, apart from the category of practice and usability, in all other categories, the level of agreement of employees from the non-profit sector was high. The employees in the concerned sector knew more about BYOD and performed more business tasks in this domain. Employee satisfaction in this sector regarding BYOD was high, while the level of satisfaction of the government employees was medium and in the private sector was low. The private sector employees also had low knowledge and usage of BYOD in business tasks, while it was medium for these factors among government employees.

Fig. 4. Factors associated with the employee perceptions regarding BYOD

In terms of risk awareness, interest in, as well as the adoption of similar trends, could be observed, where the level of agreement of the employees of the non-profit sectors has been high and those of the government sectors showed a medium level of interest, risk awareness, and adoption of BYOD. The level of interest and risk awareness regarding BYOD as well as the adoption of the same was low among employees in the private sector, as is evident from the table.

Table 1. Summarizing the findings of the survey and descriptive statistics

N	Factor	Variable Sector	Mean	Sample size	Mode	Standard Deviation	Level
1	Knowledge	Government	0.8027	679	1	0.3983	Medium
		Private	0.7273	132	1	0.4471	Low
		Non-profit	0.8612	36	1	0.3507	High
2	Practice and usability	Government	0.2062	679	0	0.4049	Medium
		Private	0.2652	132	0	0.4431	High
		Non-profit	0.1945	36	0	0.4014	Low
3	Business tasks	Government	0.5375	552		0.126	Medium
		Private	0.4165	130	N/A	0.1141	Low
		Non-profit	0.5902	36		0.0801	High
4	Employee satisfaction	Government	3.4764	679	4	1.1088	Medium
		Private	3.4289	132	4	1.1369	Low
		Non-profit	3.9161	36	4	0.7928	High
5	Risk awareness	Government	4.2725	679	5	0.7908	Medium
		Private	4.262	132	5	0.7925	Low
		Non-profit	4.4048	36	5	0.7362	High
6	Interest	Government	3.5469	679	5	1.114	Low
		Private	3.6727	132	5	1.1971	Medium
		Non-profit	3.8956	36	5	1.1409	High
7	Adoption	Government	3.1504	679	5	1.289	Medium
		Private	2.7647	132	5	1.4418	Low
		Non-profit	3.8332	36	4	0.9856	High
8	Policies and legislation	Government	4.0526	679	5	0.8948	Medium
		Private	3.7352	132	5	1.1819	Low
		Non-profit	4.4207	36	5	0.654	High

The policies and legislations in this domain are also robust in the non-profit sectors while in the case of the government it is medium and low in the private sectors. The explanations behind enhanced employee performance in the non-profit sector in the domain of BYOD has been provided in the discussion section of this paper.

The findings from the concerned survey and the numbers in the above-mentioned results table indicate the importance of considerable awareness generation and implementation of frameworks and policies to facilitate useful incorporation of BYOD, especially to mitigate problems of security and safety of organizational information and aspects of unethical incorporations [56]. This can be seen to be especially true in the case of employees in the government and private sectors. All these indicate the importance of the innovation adoption process that has been suggested in this study. These aspects have been described and put forward in the discussion section.

6. Discussion

Based on the results from the survey and analysis of the information collected from the same, a comprehensive discussion about the issue of concern has been conducted in this section. The discussion has been developed by the

research questions and objectives of the paper. The primary emphasis has been on the Innovation Adoption Process regarding the adoption of BYOD in the present period in different sectors of Saudi Arabia and also on the performance of the employees from each identified sector in each stage and the comprising elements of the stages of the innovation adoption process. Based on the same, in the later discussion, insights have been developed regarding the performance of the public, private, and non-profit sectors in the domain of BYOD and the stages of the innovation adoption process in which these three sectors in Saudi Arabia currently operate. The questions that have been addressed in this study are the following:

- What are the factors affecting the attitudes of users and organizations toward BYOD?
- How do these factors influence the adoption of BYOD among the government, non-profit, and private sectors in Saudi Arabia?
- How has BYOD been adopted by consumers in Saudi Arabia?
- What are the differences among the government, non-profit, and private sectors in Saudi Arabia regarding the adoption of BYOD, and what have suggested ways to increase the appropriate adoption of BYOD?

6.1 Innovation Adoption Process

The process of innovation adoption in any domain can assume immense importance with the constant development of technologies and innovations and their usage and applications in different spheres of human life. The process shows the different stages of adoption of a particular innovation or a change in operational process among its users, based on the level of awareness of the innovation and willingness to accept it, which can be a technology, an idea, or a change operational process [55]. The stages in the domain of the Innovation Adoption Process can be shown in Fig. 5.

The Innovation Adoption Process as discussed and presented in **Fig. 5** is used to incorporate innovation and technology in different spheres of operations and especially in professional scenarios to incorporate changes according to desired changes and dynamics in the organizational framework.

In the present research, this is of immense importance and relevance given that the study emphasizes the level and extent of awareness and usage of BYOD (an innovative practice in the professional scenarios gaining popularity, especially in the current COVID-19 pandemic situation), and also its current adoption by employees in different sectors in Saudi Arabia. Thus, the steps of the process of adoption of innovation are of immense importance in this domain and therefore in this research.

Different studies in different domains incorporate the components and stages of the Innovation Adoption Process in the domains of professional activities and customer behavior. For instance, in their extensive research paper, [52] highlighted the incorporation of the Innovation Adoption Process to examine the adoption of the concept and usage of e-wallets among consumers. The findings of this paper highlight critical factors in each stage of the innovation adoption framework concerning technological innovation, thereby helping develop suitable and robust recommendations by the authors. These assertions are similar to those of [53] who also highlighted the incorporation of the Innovation Adoption Process in the domain of mobile wallets, especially emphasizing consumers in Finland.

The Innovation Adoption Process discussed in the above section is strongly relevant to this study for the following reasons:

- It will help in assessing the stages in which the employees of different sectors currently exist in the aspects of adoption of the BYOD framework.
- It will also help in assessing the level of awareness among employees in different sectors regarding usage and security issues incorporated in BYOD.
- The steps of the concerned innovation adoption process will also help in understanding the problems in different sectors in the adoption of BYOD and also the comparison of the situations in each sector.

Taking into consideration the incorporation of the Innovation Adoption Process in different sectors, as mentioned in previous studies, the same has also been incorporated in the concerned study. It has helped understand and explain the stages in which each of the three sectors in Saudi Arabia currently operates in terms of adoption, usage, and awareness of BYOD, which in turn can help to understand security implications and thereby develop recommendations in this domain. Based on the above discussion and the results table, the stages for each of the three sectors and their implications are discussed in this section of the concerned paper.
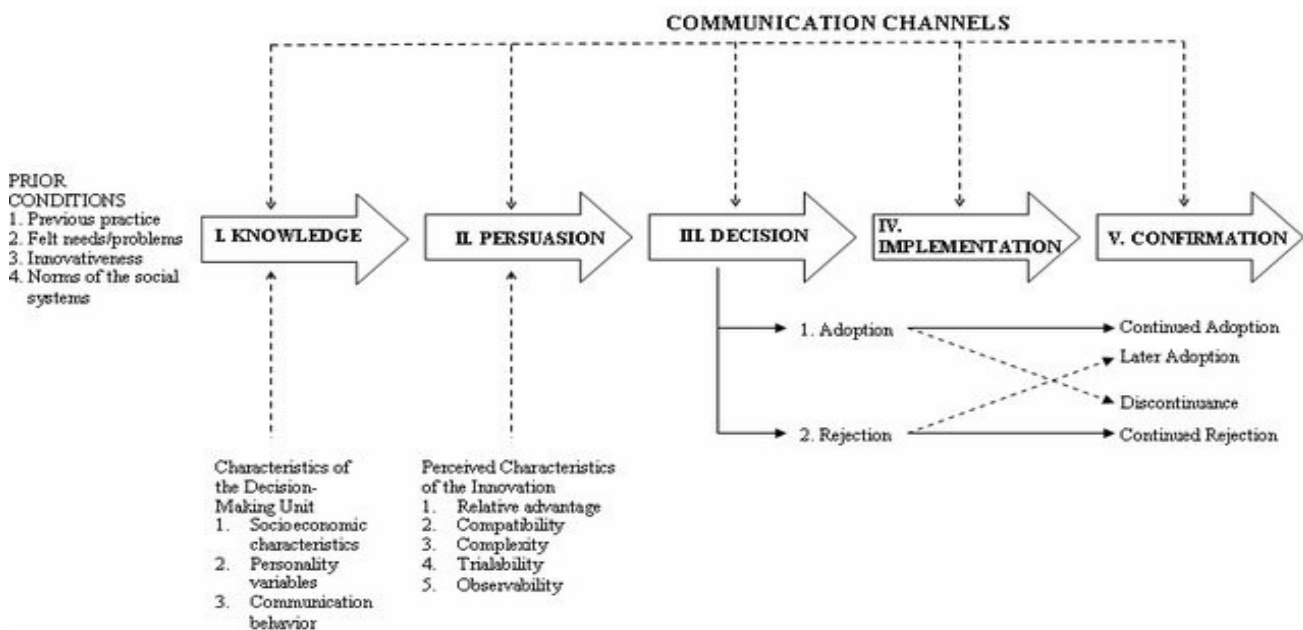

Fig. 5. Stages incorporated in the Innovation Adoption Process [55]

6.1.1 Stage 1: Knowledge Stage

For the adoption of any innovation in general and BYOD in particular, the first stage is that of the stage of development of robust knowledge among users regarding the concerned technology or innovation and its importance. The element or factor from the above table that has been considered in this stage is as follows:

- **Knowledge**
  This factor has tried to analyze the extent to which employees in different sectors in Saudi Arabia know about the incorporation, usage, and importance of BYOD and the extent to which they are using them in their professional operations. As is evident in the above table summarizing the results obtained from the information analyses of the survey, it is clear that knowledge regarding BYOD is considerably high among non-profit organization employees as compared to the medium level of knowledge among employees in the government sector and low knowledge among those in the private sector. The right stage, in this case, would have been high knowledge for employees in all sectors for proper incorporation of BYOD and also ruling out the possibility of security threats associated with the same. The reason for high knowledge among non-profit sector employees can be attributed to the smaller size and well-developed interconnectivity among non-profit organizations as compared to organizations in the other sectors. Additionally, the employees who work partly in such organizations bring information and knowledge about technologies and best practices from other sectors, thereby contributing to effective knowledge development in employees of the concerned sector. This highlights the need for more knowledge development regarding BYOD among employees in the private and government sectors.

6.1.2 Stage 2: Persuasion Stage

This is the stage where the potential users of an innovation seek more information to develop more openness and interest in the implementation of the idea or innovation. In the case of the adoption of BYOD innovation among employees in different sectors in Saudi Arabia, the elements or factors in this stage can be shown as follows:

- **Interest**
  The concerned element or factor as visible in the results table highlights the interests of employees in different sectors in the domain of BYOD as an alternative to the provision of computers or devices by the companies to concerned employees. As evident from the results table, the interest in BYOD is high among employees in the non-profit sectors, while the interest is medium in the private sector and low in the

government sector. The presence of high interest among the non-profit sector employees in Saudi Arabia is that the concerned sector and its employees operate with constrained resources, which increases their interest in adopting and using the concerning innovation, especially in the currently ongoing COVID-19 pandemic. On the other hand, there is less motivation among employees in the private sector, as they expect their organizations to provide them with needed devices and technologies.

6.1.3 Stage 3: Decision Stage

In this stage, the user or the adopter needs to make a decision based on the pros and cons of the innovation to reject or accept it. The different factors in this domain are as follows:

- **Employee Satisfaction**
  The level of satisfaction among employees in the non-profit sector is high compared to the level of satisfaction with BYOD among employees in the government and private sectors. Since the non-profit sector is small and well-connected, the establishment of the concerned innovation can be seen to be easier and more convenient in the concerned sector as compared to the private and government sectors [49]. This in turn can indicate greater importance for the other sectors to enhance the satisfaction level of their employees with BYOD usage in their jobs. It is natural for the non-profit sector of the concerned country and its employees to be satisfied with the incorporation of BYOD because they implement and use it directly and perceive the differences in comparison to other sectors due to the robust interconnection of this sector.

- **Risk Awareness**
  This factor highlights the level of awareness among employees of different sectors regarding the risks of BYOD, and per the results of this study, it is also high among non-profit sector employees, while it is medium among employees in the government sector and low among those in the private sector. This can also be attributed to the well-connected employee network and knowledge management in the non-profit sector. Additionally, the assets and resources in the public and the private sectors in the concerned country are larger than those in the non-profit sector, and this makes it more difficult for the concerned sectors to manage their resources and share knowledge effectively.

- **Policies and Legislation**
  This factor highlights existing policies and legislation in the domain of consumption of BYOD, and the robustness of these policies and laws is high in the non-profit sector, while in the private sector there are weak policies, and robustness is medium in the

government sector. The non-profit sector is considerably small, and it is thus easy to manage operations in the concerned sector, and it is also easy to develop and implement comprehensive policies and legislation [49]. This is not the case for the other sectors, which are considerably larger and more dynamic.

6.1.4 Stage 4: Implementation Stage

- **Practice and Usability**
  The concerning factor highlights the extent to which people use BYOD in their daily lives in their jobs, which is low among non-profit organizations and medium in the government sector, and the same is high in employees in the private sector. This can also be attributed to the considerable scope of implementation of BYOD in the private sector, while there are problems in knowledge development and motivation for employees regarding practice and usability of BYOD in work-related activities in the other sectors. This can be because different public and private companies provide mobile devices to their employees, and this becomes a part of their daily work. This contributes to the logical interpretation of the concerned result.

- **Business Tasks**
  For non-profit sector employees, the application of BYOD to business tasks is high, while it is low for private-sector employees and medium for government employees. Due to the presence of higher knowledge of the usability of BYOD among employees in the non-profit sector, the applications in business tasks are high among employees in the concerned sectors, while in other sectors the applicability is not that high in this case [35]. This is especially relevant in the present period due to the ongoing COVID-19 pandemic, where due to remote working set-ups, the importance of BYOD is increasing.

6.1.5 Stage 5: Confirmation Stage

In this stage, the final decision regarding the adoption of BYOD is made by employees in different sectors. As evident from the results table, the level of adoption of BYOD technology is high among non-profit sector employees, while adoption is low among employees in the private sector and medium in the government sector. This can also be attributed to the high level of knowledge and information inflow in the non-profit sector, which is also easier to manage compared to the private and government sectors [35]. Also, the presence of limited resources in the non-profit sector leads to more motivated employees in the concerned sector to adopt BYOD technology efficiently.

Based on the above discussion, it can be asserted that the employees in the private sector and the government sector are in the first stage of the Innovation Adoption Process for BYOD for work purposes. However, the employees in the non-profit sector have mostly passed the first stage and are currently in the second stage. Based on the analysis of the stages of the Innovation Adoption Process for BYOD in each sector of Saudi Arabia, the suggestions for each sector to proceed further can be developed based on the following 5-Step Solution Model as shown in Fig. 6:
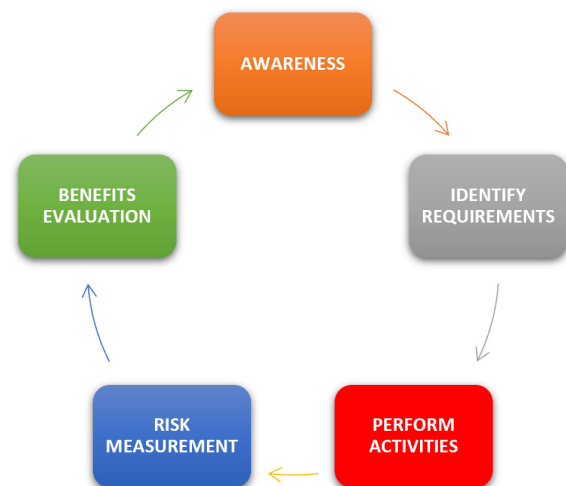

Fig. 6. 5-Step Solutions Model [56]

- For those in the private sector, it is of immense importance to develop proper awareness of usage, importance, and risks associated with BYOD and the potential benefits that can be derived from the same.
- For employees in the government sector, there is medium awareness and identification of requirements, and with more emphasis on these attributes, the concerned sector can move towards the performance of activities through the use of BYOD.
- The employees in the non-profit sector can be seen to have considerable knowledge as well as usage of BYOD in performing different work-related activities, and the concerned sector can thus move towards identification of the security risks associated with the usage of the same and thereby manage risks efficiently.

7. Implications

The findings of the concerned study have considerable importance, as they highlight the current stages of the innovation adoption process in which each sector in Saudi Arabia is operating in the present period. The different factors in each stage highlight the extent of progress of

employees across three different sectors and appropriate conditions for each of the stages. This also helps in understanding key areas of improvement that have to be emphasized by each sector for efficient incorporation and usage of BYOD, and also for mitigating security threats existing in this domain [56].

However, one limitation of this study is that it emphasizes a distinctly small sample, and the number of factors incorporated in assessing the performance of a sector in the innovation adoption process regarding BYOD is also low. This highlights the presence of threats of exclusion of crucial information, which may have led to the generalization of the outcomes to some extent. Thus, a more comprehensive and in-depth analysis of the incorporation of BYOD and the security risks for each sector separately is of immense importance to future studies in the concerned domain.

8. Conclusion

This study has emphasized assessing the incorporation of BYOD in work activities for employees in different sectors of Saudi Arabia, especially taking into consideration the importance of this innovation in the remote working environment due to the currently ongoing COVID-19 crisis. The study also tries to analyze awareness of security threats in this domain and the usability and adoption level of this innovation among employees in different sectors. From the findings of this study, it can be summarized that there currently exist considerable gaps in the awareness and adoption of BYOD in the private and government sectors, although the non-profit sector is performing effectively. The study also tries to develop robust recommendations for each sector to move toward the next stage.

Based on the limitations of this study, it can be highlighted that there is considerable room for future works in this domain, especially in investigating the general factors that influence the adoption of BYOD in the private and government sectors of Saudi Arabia in the current period and the near future. There is also room for more extensive studies in the domain of expansion of factors affecting security and privacy in the incorporation of BYOD in government sector operations in the concerned country, and future studies can also emphasize how these privacy and security issues in this domain can be substantially mitigated.

Acknowledgments

References

[1] D. Goerzig and T. Bauernhansl, "Enterprise architectures for the digital transformation in small and medium-sized enterprises," Procedia Cirp, vol. 67, pp. 540-545, 2018

[2] C. Matt, T. Hess, and A. Benlian, "Digital transformation strategies," Business & Information Systems Engineering, vol. 57, no. 5, pp. 339-343, 2015.

[3] Braña, F. J. (2019). A fourth industrial revolution? Digital transformation, labor and work organization: A view from Spain. Journal of Industrial and Business Economics, 46(3), 415-430.

[4] S. C. o. Economic and D. Affairs, "Saudi vision 2030," 2016.

[5] R. Palanisamy, A. A. Norman, and M. L. Mat Kiah, "BYOD policy compliance: Risks and strategies in organizations," Journal of Computer Information Systems, pp. 1-12, 2020.

[6] SDAIA. (2021), SDAIA Achievements. Retrieved on April 16, 2021 from https://sdaia.gov.sa/files/2020Achievements.pdf

[7] S. Bartsch, E. Weber, M. Büttgen, and A. Huber, "Leadership matters in crisis-induced digital transformation: how to lead service employees effectively during the COVID-19 pandemic," Journal of Service Management, 2020.

[8] Cook, I. (2012). BYOD – Research findings released. Retrieved on April 16, 2021 from https://cxounplugged.com/2012/11/ovum_byod_research-findings-released/

[9] K. Almarhabi, K. Jambi, F. Eassa, and O. Batarfi, "Survey on access control and management issues in cloud and BYOD environment," International Journal of Computer Science and Mobile Computing, vol. 6, no. 12, pp. 44-54, 2017.

[10] Njoroge, P., & Pazarbasioglu, C. (November 5, 2020)., Bridging the Digital Divide to Scale Up the COVID-19 Recovery

[11] A. Ghosh, P. K. Gajar, and S. Rai, "Bring your own device (BYOD): Security risks and mitigating strategies," Journal of Global Research in Computer Science, vol. 4, no. 4, pp. 62-70, 2013.

[12] C. Z. Tu, J. Adkins, and G. Y. Zhao, "Complying with BYOD security policies: A moderation model based on protection motivation theory," Journal of the Midwest Association for Information Systems (JMWAIS), vol. 1, pp. 11-28, 2019.

[13] Fiorenza, P. (2013). Mobile technology forces study of bring your own device. Public Manager, 42(1), 12.

[14] El Gbouri, A., & Mensch, S. (2020). Factors affecting information security and the widest implementations of Bring Your Own Device (BYOD) programs. ACET Journal of Computer Education & Research, 14(1).

[15] K. Downer and M. Bhattacharya, "BYOD security: A new business challenge," in 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), 2015, pp. 1128-1133: IEEE.

[16] Jamal, F., Taufik, M., Abdullah, A. A., & Hanapi, Z. M. (2020, April). A systematic review of Bring Your Own Device (BYOD) authentication technique. Journal of Physics: Conference Series, 1529(4), 042071. IOP Publishing.

[17] Lenovo Tech Today (2021). Is the public sector letting BYOD down? Retrieved on April 16, 2021 from https://techtoday.lenovo.com/sa/en/solutions/smb/public-sector-letting-byod-down

[18] BYOD. (25 August 2020). Mobile device guidance Retrieved on April 16, 2021 from

https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device

[19] Kang, Q., Xue, L., Morrison, A., Tang, Y., Chen, A., & Luo, X. (2020). Programmable in-network security for context-aware {BYOD} policies. In 29th {USENIX} Security Symposium ({USENIX} Security 20) (pp. 595-612).

[20] Microsoft 365 (03/27/2021). Protect unmanaged Windows 10 PCs and Macs Retrieved on April 17, 2021 from https://docs.microsoft.com/en-us/microsoft-365/campaigns/m365-campaigns-protect-pcs-macs?view=o365-worldwide&tabs=Windows10

[21] Al-Harthy, I. M., Rahim, F. A., Ali, N. A., & Singun Jr., A. P. (2020). Dimension of Protection Behaviors: A Systematic Literature Review. Journal of Theoretical and Applied Information Technology, 98(17).

[22] Blagden, R. J. (2020). An implementation strategy for Bring Your Own Device in the NHS: An innovation study (Doctoral dissertation, Imperial College).

[23] The relation between the public and private sector. Retrieved on April 17, 2021 from http://dr-ama.com/

[24] Alghamdi, J., & Holland, C. (2020). A comparative analysis of policies, strategies and programmes for information and communication technology integration in education in the Kingdom of Saudi Arabia and the republic of Ireland. Education and Information Technologies, 25(6), 4721-4745.

[25] Irvin, R. (2017) Non-profit organization. Retrieved on April 17, 2021 from https://www.britannica.com/topic/nonprofit-organization/additional-info%23contributors

[26] Dincer, I., Hussain, M. M., & Al-Zaharnah, I. (2004). Energy and exergy use in public and private sector of Saudi Arabia. Energy Policy, 32(14), 1615-1624.

[27] Alirezabeigi, S., Masschelein, J., & Decuypere, M. (2020). Investigating digital doings through breakdowns: A sociomaterial ethnography of a Bring Your Own Device school. Learning, Media and Technology, 45(2), 193-207.

[28] Alghamdi, A. (2018) The degree of importance of the partnership between the University of Jeddah and the private sector in light of the vision of the Kingdom of Saudi Arabia 2030.

[29] Essa, Mohammed Abdel A'al Dr (2018) "Partnership between the Public and Private Sectors: Concept, Reasons, Motivation and Perspectives," Arab Journal of Administration: Vol. 38 : No. 3 , Article 2.

[30] 2030 vision. (2021). National Transformation Program. https://www.vision2030.gov.sa/v2030/vrps/ntp/

[31] 2030 vision. (2021). National Transformation Program – Acting Plan. http://www.arabia-saudita.it/files/pages/2014/05/ntp_en.pdf

[32] Austin, G. (Ed.). (2020). Cyber security education: Principles and policies. Routledge.

[33] Namaa Portal (2021). Non-Profit Services Portal. Retrieved on April 17, 2021 from https://namaa.sa/

[34] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and privacy considerations," It Professional, vol. 14, no. 5, pp. 53-55, 2012.

[35] B. Alotaibi and H. Almagwashi, "A Review of BYOD security challenges, solutions and policy best practices," in 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), 2018, pp. 1-6: IEEE.

[36] M. M. Singh, C. W. Chan, and Z. Zulkefli, "Security and privacy risks awareness for bring your own device (BYOD) paradigm," International Journal of Advanced Computer Science and Applications, vol. 8, no. 2, pp. 53-62, 2017.

[37] B. Morrow, "BYOD security challenges: control and protect your most sensitive data," Network Security, vol. 2012, no. 12, pp. 5-8, 2012.

[38] M. Dhingra, "Legal issues in secure implementation of bring your own device (BYOD)," Procedia Computer Science, vol. 78, pp. 179-184, 2016.

[39] O. Ehikioya, A. P. Binitie, and A. Joe-Obasi, "SECURITY RISKS ASSOCIATED WITH BRING YOUR OWN DEVICE BYOD AND POSSIBLE MITIGATION TECHNIQUES," SOUTH EASTERN JOURNAL OF RESEARCH AND SUSTAINABLE DEVELOPMENT (SEJRSD), vol. 2, no. 1, pp. 148-165, 2019.

[40] K. Almarhabi, K. Jambi, F. Eassa, and O. Batarfi, "A Proposed Framework for Access Control in the Cloud and BYOD Environment," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 2, pp. 144-152, 2018.

[41] K. Almarhabi, K. Jambi, F. Eassa, and O. Batarfi, "An Evaluation of the Proposed Framework for Access Control in the Cloud and BYOD Environment," INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, vol. 9, no. 10, pp. 213-221, 2018.

[42] De Kock, R., & Futcher, L. A. (2016). Mobile device usage in higher education institutions in South Africa. 2016 Information Security for South Africa (ISSA) (27-34). IEEE.,

[43] Yeop, Y. H., Othman, Z. A., Abdullah, S. N. H. S., Asma'Mokhtar, U., Fauzi, W. F. P., & Ahmad, N. (2018). Key factors to implement BYOD in schools. 2018 Cyber Resilience Conference (CRC) (1-3). IEEE.

[44] Yeop, Y. H., Othman, Z. A., Abdullah, S. N. H. S., Mokhtar, U. A., & Fauzi, W. F. (2018). BYOD implementation factors in schools: A case study in Malaysia. Int. J. Adv. Comput. Sci. Appl., 9(12), 311–317, 2018,

[45] Othman, Z., Sepli, M., Mokhtar , U., & Yeop, Y., (2020). BYOD implementation model in Malaysian schools: The perception and readiness of parents, schools, and teachers. Int. J. Adv. Appl. Sci., 7(6), 57–68.

[46] Musarurwa, S., Gamundani, A. M., & Shava, F. B. (2019, May). An assessment of BYOD control in higher learning institutions: A Namibian perspective. In 2019 IST-Africa Week Conference (IST-Africa) (1-9). IEEE.

[47] Cheng, G., Guan, Y., & Chau, J. (2016). An empirical study towards understanding user acceptance of bring your own device (BYOD) in higher education. Australasian Journal of Educational Technology, 32(4).

[48] Musarurwa, A., Flowerday, S., & Cilliers, L. (2019). The bring-your-own-device unintended administrator: A perspective from Zimbabwe. The Electronic Journal of Information Systems in Developing Countries, 85(4),

[49] H. Chen, Y. Li, L. Chen, and J. Yin, "Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security–related conflict and fatigue," Journal of Enterprise Information Management, 2020.

[50] T. Alhussain, R. AlGhamdi, S. Alkhalaf, and O. Alfarraj, "Users" Perceptions of Mobile Phone Security: A Survey Study in the Kingdom of Saudi Arabia," international journal

of computer theory and engineering, vol. 5, no. 5, p. 793, 2013.

[51] Alsayed, Nemah & Alakel, Haifaa & Mohammed, Ferdous. (2016). Privacy and Social Networking: WhatsApp Users' Perception in Saudi Arabia.

[52] Alfina, S. M. (2020, June). From Physical to digital: Consumer adoption process to e-Wallet. In 23rd Asian Forum of Business Education (AFBE 2019) (15-21). Atlantis Press.

[53] Doan, N., 2014. Consumer adoption in mobile wallet: A study of consumers in Finland. [online] Available at: https://www.theseus.fi/bitstream/handle/10024/86343/Ngoc _Doan.pdf?sequence=l

[54] Dribbisch, K., 2017. Translating innovation: The adoption of design thinking in a Singaporean Ministry.

[55] Rogers, E. M. 1995. Diffusion of Innovations. 5th ed. New York: Simon and Schuster.

[56] Omokehinde, S.O., 2019. Factors to consider when developing an organisation-wide bring your own device (BYOD) strategy for adoption.

[57] Smith-Ditizio, A. A., & Smith, A. D. (2018). BYOD (Bring Your Own Device), mobile technology providers, and its impacts on business/education and workplace/learning applications. In Encyclopedia of Information Science and Technology, Fourth Edition (5981-5991). IGI Global.

AHMED MOHAMMED ALGHAMDI is an assistant professor at the Software Engineering Department, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia. He got his Ph.D. in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia. He received his B.Sc. degree in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia, in 2005 and the first M.Sc. degree in Business Administration from King Abdulaziz University, Jeddah, Saudi Arabia, in 2010. He received the second master's degree in Internet Computing and Network Security from Loughborough University, UK, in 2013. Dr. Ahmed also has over 11 years of working experience before attending the academic carrier. His research interests include high-performance computing, big data, distributed systems, programming models, software engineering, BYOD, and software testing.

ADEL A. BAHADDAD received the B.S. degree in computer science from Science's College, Saudi Arabia, in 2002, and the M.S. and Ph.D. degrees in information and communication technology from the School of Information and Communication Technology, Griffith University, Brisbane, Australia, in 2012 and 2017, respectively. He is currently an Assistant Professor with the Faculty of Computing and Information Technology, King Abdulaziz University (KAU), where he serves Head of the Department of Systems and Educational Programs at the Deanship of E-Learning and Distance Education (Since 2018). He participated in a number of executive committees concerned with automating operations at the Educational Curriculum Center and the Strategic Plan of the Strategic Center to achieve the Kingdom's vision at King Abdulaziz University. His research interests area include diffusion and technology adoption and Digital Transformation, M-Service, M-Commerce, LMS, and M-Governances., BYOD And he has many publications in these fields.

Khalid Ali Almarhabi is an assistant professor at the Computer Science Department, College of Computing in Al-Qunfudah, Umm Al-Qura University, Saudi Arabia. He got his Ph.D. in Computer Science after studying this degree at both King Abdulaziz University, Jeddah, Saudi Arabia, and Queensland University of Technology, Brisbane, Australia. He also holds an MSc degree in Information Technology from Queensland University of Technology, Brisbane, Australia, in 2014. He holds a BSc degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia, in 2009. His research interests are information security, BYODs research, access control policies, information system management, and cloud computing.