Adoption of the Bring Your Own Device (BYOD) Approach in the Health Sector in Saudi Arabia

Khalid A. Almarhabi [1*], Ahmed M. Alghamdi [2], and Adel A. Bahaddad [3]
[1] Department of Computer Science, College of Computing in Al-Qunfudah, Umm Al-Qura University, Makkah 24381, Saudi Arabia
[2] Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 21493, Saudi Arabia
[3] Department of Information System, Faculty of Computing and Information Technology, King Abdulaziz University Jeddah 21589, Saudi Arabia
*Corresponding author: Khalid A. Almarhabi; kamarhabi@uqu.edu.sa

Summary
The trend of Bring Your Own Device (BYOD) is gaining popularity all over the world with its innumerable benefits such as financial gain, greater employee satisfaction, better job efficiency, boosted morale, and improved flexibility. However, this unstoppable and inevitable trend also brings its own challenges and risks while managing and controlling corporate data and networks. BYOD is vulnerable to attacks by viruses, malware, or spyware that can reach sensitive data and disclose information, modify access policies, disrupt services, create financial issues, minimise productivity, and entail some legal implications. The key focus of this research is how Saudi Arabia has approached BYOD with the help of their 5-step solution model and quantitative research methodology. The result of this study is a statement about what users know about this trend, their opinions about it, and suggestion to increase the employee awareness.

Keywords:
Bring Your Own Device (BYOD), information management, Saudi Arabia

1. Introduction

Nations all over the globe are trying to achieve digital transformation to help them enhance their strategic goals and services. The process of digital transformation helps in changing the business model of the private sector or government companies into a new model based on digital technologies for providing services, manufactured products, and management of human resources [1]. The basic aim of digital transformation is to upgrade business models to stay aligned with ongoing technological developments, boost operational efficiency, and minimise errors [2]. It also plays an important role in enhancing customer and employee satisfaction, increasing revenue, and inspiring innovation [3]. The World Competitiveness Centre of the Institute for Management Development (IMD) in Lausanne, Switzerland has created a digital indicator (Digital Competitiveness Index) to assess this competition and show the digitalization rankings of countries across the world.

When the COVID-19 pandemic struck, it pressured the communication sector to look beyond traditional means of communication to seek information. This sector is actually the backbone that guides the usage of data, digital applications, and content by individuals, companies, and governments to ensure that social and economic activities continue despite closure and social distancing in many countries [4]. Saudi Arabia has unexpectedly used the pandemic as an opportunity to accelerate its digital transformation process comprising of incentives for advanced electronic transactions that motivate private and governmental institutions to offer digital services, which are acceptable and satisfactory to the public [5].

The government of Saudi Arabia has supported the digital transformation process in several ways. Firstly, Saudi Arabia has a vision for 2030 in which the government is trying to provide shared services for all their government agencies [6]. This will help in achieving better productivity and justifying spending. These shared services will aim to increase quality, minimise costs, consolidate efforts, and create a positive work environment for everyone. As per this vision, the government of Saudi Arabia will support the implementation of online applications in all government agencies like cloud applications, HR management systems, and data-sharing platforms. Secondly, the goal behind creating the Supreme Royal Decree number 7/B/33181, dated 7 September 2003, was a complete transformation of Saudi Arabia into an information and technology society based on a plan to provide electronic access to government services [7]. Lastly, Saudi Arabia is a member of the G20, which aims to bring together important developing and industrialised economies for discussing important global issues. The most important agenda item of the G20 is to focus on digitisation, which aims to convert information into a computer-readable digital format, requiring the organisation of information into bits [8].

There are different ways to achieve digital transformation, and one of the most suitable is the Bring Your Own Device (BYOD) approach. This approach

Manuscript received July 5, 2022
Manuscript revised July 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.7.46

requires employees to use their personal devices to connect to their organisation's network and systems [9]. These devices can be their smartphones, tablets, USB drives, or personal computers. The concept of BYOD has become popular after CISCO adopted it in 2009 [10], and its adoption has also been fuelled by IT consumerism. Employees are largely permitted by their employers to use their personal mobile devices due to their advanced features. There are various advantages of BYOD such as reducing costs and boosting user productivity. Some additional benefits are savings in procurement, software, hardware, service agreements, insurance, and licensing [11]. Some of the reasons for implementing BYOD are enhanced employee mobility, productivity, satisfaction, and flexibility. A few aspects must be considered while deploying BYOD. First, BYOD boosts efficiency, as every employee is an expert in using their own personal devices, which minimises the need for training [12]. Second, it helps in providing services at minimum cost, even in rural areas. Third, employees who use their own devices are quite diligent in doing so [13]. Finally, information sharing and communication is instantaneous and can be accessed from anywhere, even without LAN or Wi-Fi availability [14].

However, several challenges must also be addressed while adopting BYOD. Some of the drawbacks faced by employees while using their personal device at their workplace include data breaches if the personal device of the employees is stolen or lost. Challenges also include the absence of protection setups like antivirus software or firewall on personal devices. Increase in IT cost while supporting personal devices is another challenge, and finally lack of management and network control in BYOD devices [15-17].

The basic objective of this research is to investigate issues linked to the implementation of BYOD in health sector in Saudi Arabia. Some of the key issues are higher inherent risks, increasing attacks because of poor control of individual devices by the data administrator, shadow IT, employees downloading malicious apps, and everyone not being ready to adopt the concept. There are a number of factors affecting the regional development for Information and Communications Technology (ICT); some have a direct impact, while others might have an indirect impact. ICT regional development can be a challenging situation and should be considered from a multi-dimensional perspective. Strategy and vision, privacy and security legislation, leadership roles, top management support, organisational culture, change management, education and awareness, and overall ICT infrastructure differ from one area to another. Varying regulatory environments, workplace practices, and culture can result in unusual difficulties. Thus, this study is aimed at the Saudi Arabian audience in its objective of investigating the BYOD status in health sector in Saudi Arabia. There are four chief sub-objectives here:

1. Identify the status of the spread of this concept and its use in health sector in Saudi Arabia.
2. Investigation of users' perspectives regarding mobile devices that are personally owned and used in an organisation.
3. Investigating the attention paid by the organisation to the implementation of BYOD trends.
4. Identifying the unintended and intended usage of BYOD and the viewpoint of those who have knowledge of its trends.

The paper begins with an introduction to digital transformation, next moving on to how the audience of Saudi Arabia sees BOYD. The benefits and definitions of BYOD are then briefly explained. Next, a study of the literature and research goals and questions is provided. Data analysis and research methodology form the next part of the study and are followed by implications and discussion in the conclusion of the paper.

2. Literature Review

Few studies have been carried out in Saudi Arabia regarding this topic, and the majority of the work that has been done examines other nations. Researchers have determined the information security risks associated with BYOD in a case study of Lesotho [15]. Some other researchers have published an article entitled '"Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): The roles of information security–related conflict and fatigue" [18]. This study analyses how and whether Chinese employees have decided to implement BYOD while dealing with conflicts related to information security. The benefits of BYOD have been explained in varying papers that focus on financial gain, boosted morale, and greater satisfaction of the employees, improved job efficiency, and enhanced flexibility [19-24]. The security risks associated with BYOD have been researched on a large scale with respect to process, technology, and people based on the golden triangle model [25-30]. These challenges can be divided into four main categories: deployment, technical, regulation, and human aspects, as shown in Fig 1.

Some researchers have focused on the influence of general key concerns of BYOD [10, 17, 32, 33] in terms of four main categories. First, security associated with high possibility of factors such as device loss, device theft, and malicious attacks, which affect the entire organisation. Second, device type can make control more difficult due to different supply chains and platforms. Organisations need to enforce policies for all these different devices to prevent attacks and control employee performance. Third, the cost of controlling and managing these devices need to be

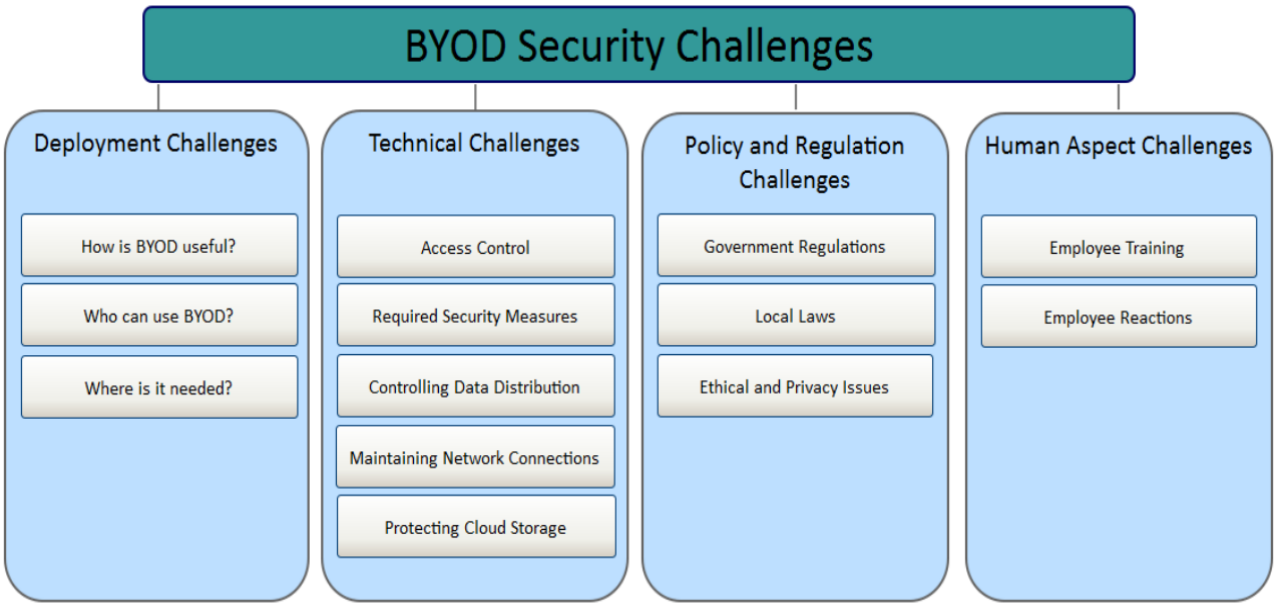


Fig. 1. BYOD security challenges [31]

considered and kept as low as possible, even with a variety of infrastructures and platforms. Finally, privacy is one of the main concerns for users in terms of how they can ensure their right to keep and share their data securely.

Some critical factors affect the success of BYOD, as explained by some authors [34-36]. Policy refers to a set of rules defined in response to an organisation's issues specifying how employees use their BYOD devices in effective and appropriate ways in the work environment while protecting their privacy. Infrastructure plays an important role in implementing BYOD successfully and refers to hardware and software that connects and controls Wi-Fi, antivirus, and Mobile Device Management (MDM). User collaboration is extremely important to the success of BYOD and the achievement of enterprise goals. Collaboration increases productivity opportunities and maintains work efficiency while employees move with their BYOD devices from location to other. Training and education in using devices in accordance with policies is important for organising work, managing the behaviour of individuals, and reducing potential risks.

Some research has been done on Saudi Arabia regarding data security and privacy from the users' point of view. Alhussain and others [37] investigated user perception about security in the mobile phone. The main result shows that users need an advanced mechanism to protect data stored in their devices through implementing a secure authentication strategy. The research did not address the issue of using these devices at work instead of company devices as in BYOD, and the paper's date of publication was near the beginning of the spread of the concept of BYOD. Alsayes and others [38] investigated WhatsApp users' perceptions of privacy regardless of the device used. The primary result was that young people are aware about privacy issues and worried about their data being accessed by third parties.

3. Research Methodology

In this section, we discuss and describe our processes for research data collection as well as methodology for proposed validation. The quantitative research method has been used in our research to explore BYOD and assess its current situation in Saudi Arabia, including terminology and usage. We chose this approach because of its ability to determine attributes and opinions of participants.

We used a survey to evaluate the respondents' understanding and awareness of BYOD. Our main concern is to understand the level of knowledge and usage and distinguish between the respondents' intended and unintended usage of BYOD. In addition, our research focuses on different aspects and variables that can affect understanding and using BYOD in health sector in Saudi Arabia. Finally, the opinions of respondents' will be discussed to gain insight into current usage, concerns, and opinions about BYOD.

The questionnaire was divided into three main components: demographic information, using a personal device for work, and BYOD. The first part is demographic information covering age, sex, education, job status, organization, device types provided by the organization, personal device types, and using personal devices in completing job tasks. The second part concerns the participants' behavior in using their own personal devices in the workplace as well as completing their work tasks

outside the workplace. Finally, the third part covers the concept of BYOD, focusing on participants who understand and have prior knowledge of this concept. In this part, the questions use a Likert scale with measurements of 1 to 5, including (1) Strongly disagree (2) Disagree (3) Neutral (4) Agree (5) Strongly Agree. We used different software to complete the surveys and analyse the data.

4. Data Analysis

As a result of the space limitations of presenting and discussing the data analytics of the research, since the questionnaire included 29 items, we focus on the more relevant results to be presented in this section. Our sample size was 857 participants, including 184 participants with prior knowledge of BYOD, which represent 21.47% of the total number of respondents indicating lack of knowledge of BYOD, although 79.46% of the participants use personal devices in their work. In terms of education level, the majority of the participants have bachelor's degrees representing 46.44%, and 25.79% have a master's degree, as shown in Fig 2. In terms of the job status of the participants, 85.65% worked in several sectors including 79.46% public-sector employees and 15.29% private-sector employees, and 4.20% worked in a non-profit organisation.

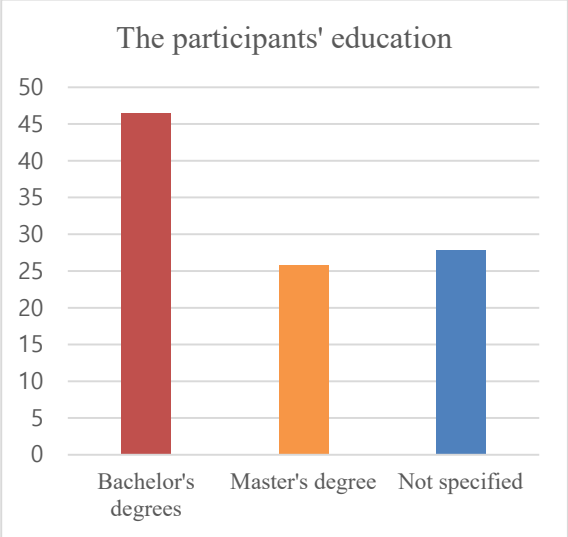


Fig 2: Participants' education level

In terms of demographic information, our study shows that the age group from 36 to 45 years old is the largest in our study, representing 46.09% of the total number of participants. The education level of the respondents shows that the Bachelor's and Master's degrees were the largest groups in our study by 46.44% and 25.79%, respectively. Despite the low number of female participants is low (13.07% of the total number), our study shows that there is a similarity in the percentages of knowledge of BYOD between males and females, as the percentages of males and females having BYOD knowledge were 21.71% and 23.42%, respectively, as shown in Fig 3.

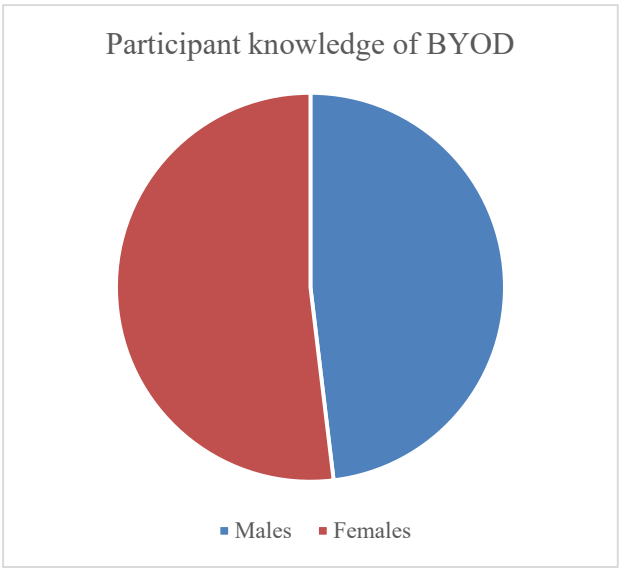


Fig 3: Participant knowledge of BYOD

In terms of BYOD-related data, the majority of participants have no prior knowledge of BYOD, representing 78.53%. Moreover, 79.46% of the participants use their devices for their work, but only 18.67% know about BYOD, which indicates a lack of knowledge that could lead to several issues related to security and privacy threats. Also, 48.66% of the respondents bring their devices to their workplaces, but only 12.37% know BYOD, which can lead to security risks. Finally, these BYOD-related data prove that there is a lack of BYOD knowledge that needs to be considered because of the rapid increase of using personal devices in the workplace, which can pose threats to individuals and organisations alike if there is no management of BYOD. This confirms the importance of organisations and related government sectors raising awareness and educating users about BYOD, digital transformation, and their effects on the relationship between users and organisations.

5. Proposed Solution

This research aims to explore and understand the current situation of BYOD in health sector in Saudi Arabia, including the level of usage of this approach for individuals and organisations. In addition, we will distinguish between the intended and unintended uses of BYOD by discovering the attributes that can affect this approach, providing insight into users' and organisations' opinions of BYOD. The main

research question tries to determine how much employees generally understand and use the concept of BYOD in health sector in Saudi Arabia. Finally, by reaching a better understanding of the current situation of BYOD, we will provide suggestions and solutions to raise awareness of BYOD's importance.

The following Fig 4 shows the proposed 5-step solution to activate the required role in raising awareness and level of acceptance for targeted segments, people, and organisations in health sector in Saudi Arabia. It is especially beneficial to develop this concept in the governmental and semi-governmental sectors because they lead various other sectors of society that can increase confidence and acceptance in the targeted environment.

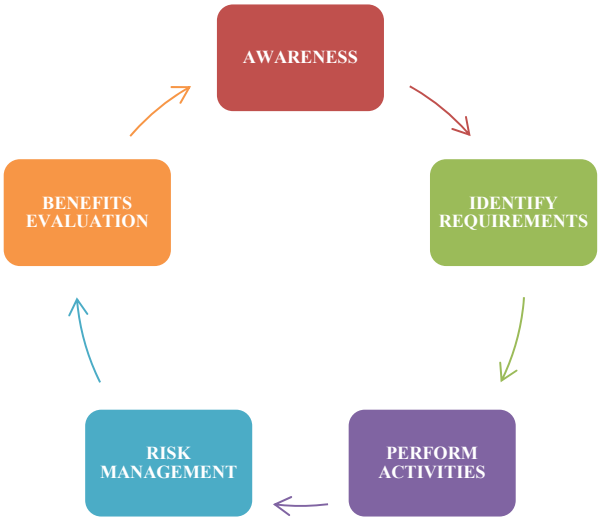


Fig 4: The proposed 5-Step solution

5.1 Awareness

The awareness in dealing with the BYOD approach represents one of the main basic aspects that can have effects in increasing the number of people to be interested in this approach, usage, development, and challenges. Thus, the awareness of BYOD should be increased in the community via several possible methods [27]. An example of these methods is to find appropriate channels to increase awareness of the benefits on the one hand and the risks on the other to integrate appropriate awareness of BYOD among users. Therefore, many questions appear at the beginning level of knowledge, as well as if there is actual use of BYOD without prior knowledge [39].

5.2 Identify Requirements

The requirements identifications represent one of the fundamental aspects of increasing the organisation's ability to move to an electronic approach, which depends on the scope of application. In our study, the survey shows that awareness of the BYOD approach and usage will increase employees' satisfaction, which will lead to an increase in productivity. Additionally, the organisations start to push towards BYOD to increase productivity. Finally, usage of BYOD will be affected either positively or negatively by providing devices from the organisation or the user.

5.3 Benefits Evaluation

Evaluation of the benefits and ensuring their existence is the most basic aspect that will increase acceptance and spread across the various government sectors. This is directly reflected in increased satisfaction for individuals and sectors seeking to implement BYOD and increasing chances of acceptance [5]. Consequently, it is important to know the tasks that users can perform with personal devices inside or outside their work hours and locations. In addition, it is important to know the benefits of using BYOD for the service sector in terms of the percentage of completed tasks, the time the tasks take, using cloud services, and applying digital transformation.

5.4 Risk Management

Digital transformation has several features and various benefits. However, these benefits and features come with risks that need to be identified, addressed, and managed using required resources. One risk associated with using the BYOD approach is that organisations have a lack of clarity, especially non-profits, in determining and identifying potential risks and difficulties before they decide to use the BYOD approach. This lack of clarity has been displayed through lack of knowledge of BYOD by a wide range of participants, as well as the lack of plans and policies needed to maintain security, confidentiality, and information availability. Therefore, risk management will play a role in the awareness of individuals and organisations of potential risks, as well as what plans and policies are in place and implemented to address these risks.

5.5 Perform Activity

Each approach, including BYOD, has a segment that will help to spread and maintain and at the same time serve as the main nucleus that will help to develop the approach until it reaches acceptance. Previous studies show the importance of providing the basic core of the BYOD approach. Therefore, defining the segment's characteristics is expected to contribute to determining these characteristics and how to use them in spreading the BYOD approach. In addition, applying basic policies will help to create a clear roadmap within the targeted segments, which will be responsible for spreading BYOD awareness.

6. Discussion

It is important to understand who lead the approach of BYOD, whether they are individuals or organisations. Our study results indicate that the use of personal devices in the workplace helps to increase productivity and is thus reflected in their performance, which increases desire to spread the approach on a wider scale. Also, the results of the questionnaire presented that 65.76% of those familiar with BYOD felt that using this approach satisfies and motivates users in their work, as shown in Fig 5. Therefore, organisations are keen to adopt this approach on a wide scale, especially with the current pandemic situation, to improve services and reengineer processes. In this part of our research, we will discuss our proposed solution associated with the results of our survey, which is related to essential aspects of the BYOD theoretical framework.

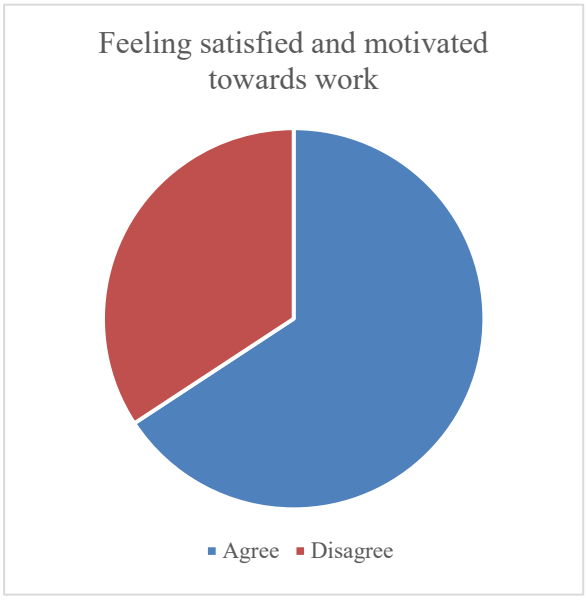


Fig 5: Feeling satisfied and motivated towards work

6.1 Awareness

The literature review showed a lack of BYOD information in the Middle East in general and Saudi Arabia in particular due to the topic's novelty on the one hand, and to a work culture that emphasises the importance of office work and coming to workplaces on the other hand [15, 18, & 23]. Therefore, the government of Saudi Arabia's move towards digital transformation emerged with the adoption of the e-government approach, starting with the Yesser program in 2005 and with the support of the Kingdom's Vision 2030. The digital transformation program was assigned to the National Information Center (NIC) and the Saudi Data and Artificial Intelligence Authority (SDAIA) to provide the needed infrastructure and to ensure collaboration between different sectors and organizations to benefit from e-government services leading to a culture of digital transformation in health sector in Saudi Arabia [40]. Different governmental sectors had various plans to support gradual digital transformation based on ambitious plans that would put Saudi Arabia in 43rd place on the United Nations scale, which measures the readiness of governments to adopt the e-government approach [41, 42].

Our survey shows that there is limited knowledge of BYOD, even for those who use technology in their daily lives, which represents only 21.47% of respondents already having prior knowledge of BYOD, as shown in Fig 6, and only 15% of respondents used their personal devices in their workplaces. Additionally, the importance of BYOD has increased in the era of the COVID-19 pandemic because of the changing situations that lead to suspending many public and private sector employees from going to their workplaces. As a result, many electronic solutions have been developed to enable employees to complete their tasks remotely in the case of curfew or their workplaces based on the general pandemic situation and the country's regulations.

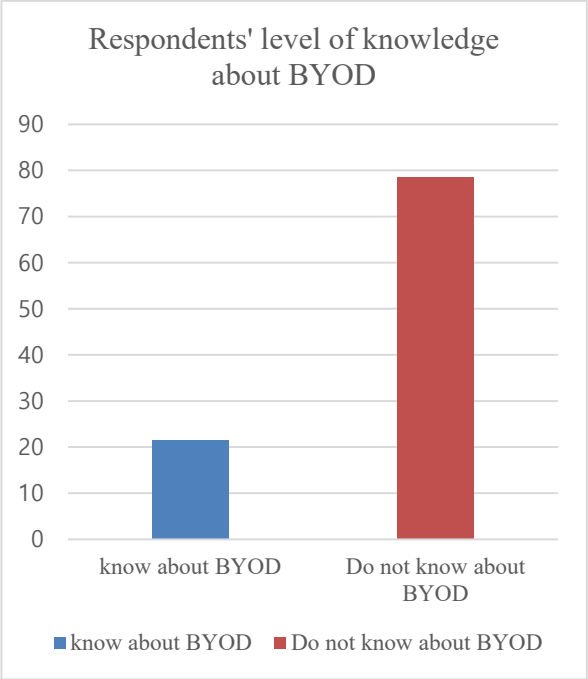


Fig 6: Respondents' level of knowledge about BYOD

In the past decade, the high use of smart devices and the availability of Internet connection has led to the use of BYOD in different aspects without having basic information about it or even the most basic and important framework to consider when applying BYOD. Our study shows that 78.53% of the respondents appear to not have known the term before, which means that usability exists but without required awareness by the targeted segment and

without organisational plans for dealing with BYOD. Consequently, awareness will greatly help to learn the basic requirements for providing a safe environment for using BYOD for both users and organisations.

6.2 Identify Requirements

Level of satisfaction is a critical factor when activating any system or technology. In our study, the results indicated that the use of personal devices to complete job tasks helps to increase productivity and is thus reflected in organisation performance, and more than 61% of employees that know BYOD believe that the use of the BYOD approach satisfies and motivates users. Therefore, organisations are keen to adopt this approach to provide better customer service experiences as well as increasing organisational efficiency. On the other hand, some respondents showed a level of resistance to using personal devices, the causes of which need to be considered and understood. Previous studies show that employees' rejection of using their devices was due to the overlap of work requirements with their personal life, as they want to avoid their work lives interfering with their personal lives. However, these studies also showed the positive side of applying the BYOD approach, which includes high flexibility for employees, especially those who have multiple missions and responsibilities. Our survey results showed that 48.66% or respondents use their devices in the workplace and 30.81% reject using them, while 20.51% did not answer this question, as shown in Fig 7. Surprisingly, 71% of the respondents used their personal devices outside the workplace to accomplish work and job tasks, and this explains the limited drawbacks of applying

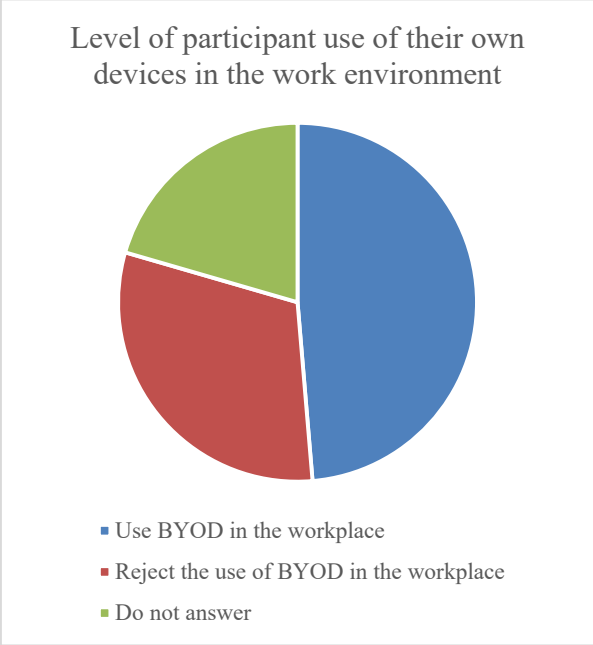


Fig 7: Level of participant use of their own devices in the work environment

this approach compared to the greater advantages that help spread it. This requires a detailed examination of these negatives to find solutions to overcome this resistance based on their sectors. Each sector might need specific technical solutions that suit their nature, which will help increase the acceptance of this approach in the future.

6.3 Benefits Evaluation

In terms of evaluating the benefit gained during the COVID-19 pandemic from BYOD, efforts have been made to provide many technical solutions as well as electronic channels to ease the community's lives. The International Monetary Fund (IMF) has cited the importance of government support in several countries to provide the appropriate mechanisms for societies to accept dealing with electronic systems. During the COVID-19 pandemic, many countries have approved cancelling many fees for government e-services, which represent basic revenues and resources in many countries such as Saudi Arabia [41]. The other benefit is to focus on providing Internet services such as 4G and 5G networks in many residential areas, as well as broadband services with various entities including residential, small, and medium-sized companies. This helps in getting various segments of society to accept digital transformation, which can be used to strengthen the BYOD approach in business, governmental, and semi-governmental institutions.

One of the challenges facing digital transformation is how to deliver digital products more flexibly and professionally. Therefore, one of the recommendations made by the IMF through the giant tech companies (Big Tech) helps in creating digital transformation with economic and technical value [41]. The COVID-19 pandemic has accelerated this process by enhancing this type of service in the life of societies, whereas the governance of global digital finance platforms helps create an appropriate environment that can be reproduced for many organisations that use technical systems in dealing with departments and users [42]. An example of these platforms on the financial side is the Apple Pay & STC Pay platforms, which is a Saudi Telecom Company offering many services and solutions with a market value of about 46.7 billion dollars [42]. These financial solutions have created a revolution in payment method, which affects both businesses and customers as well as government sectors related to financial activities. Such platforms and solutions will help provide balance and sustainable development across many sectors.

In terms of evaluating the benefits of the BYOD approach, our study shows that many job tasks are performed with computers, laptops, smartphones, and tablets. The three most important tasks, which represent the most use of personal devices, are summarised in following-up e-mail by 60% of the participants; in addition to

completing tasks and following up on them (47% and 43%, respectively) as shown in Fig 8. Consequently, organisations must adopt the technical systems in this approach, which increases productivity.

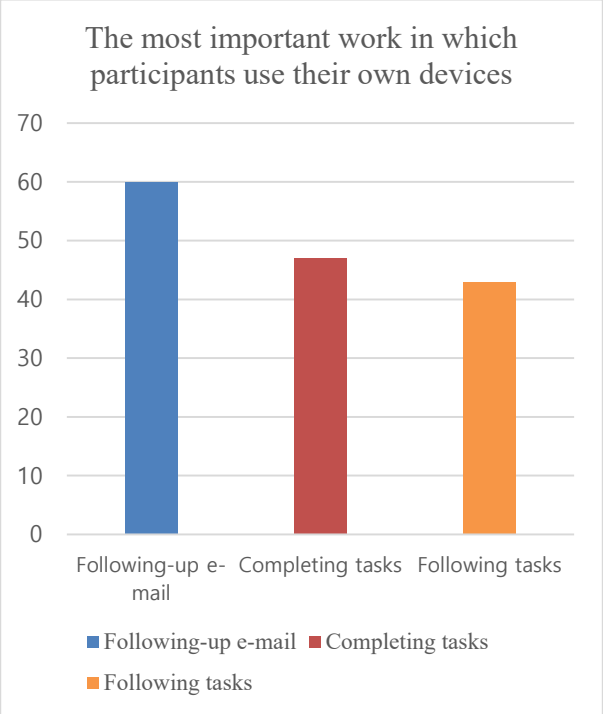


Fig 8: The most important work in which participants use their own devices

Previous studies have focused on the importance of adopting e-mail and other document management systems in dealings with government departments and the private sectors [25, 43]. Still, many sectors need high-level decisions to activate using these methods fully within the digital transformation system, which is considered one of the goals of the Kingdom's Vision 2030 and one of the outputs of the National Transformation Program 2023 [25, 26]. The adoption of these electronic methods becomes necessary as the government approach requires all government and private sectors to provide a legal entity on the Internet to include infrastructure and cybersecurity at several levels. The adoption of technical solutions has had a great impact in reversing the consequences of the pandemic that appears in several ministries that have worked to employ technology in their procedures [15, 43].

In addition, activating integration with the capabilities of the private sector provides various solutions, including clouds, to those who can benefit from them in the infrastructure required for this field [40]. We believe that the availability of infrastructure in organizations will benefit from the speed of integration of ministries and organisations in digital transformation, and this approach will the help accelerate use of the BYOD approach, whether from within or outside the organization [39, 40].

In sum, it is important to define the benefits of using the BYOD approach carefully and gradually, as those benefits have increased due to the pandemic including the acceptance of digital transformation and e-services. This leads to the importance of leveraging to embrace more in-depth benefits in the future and to help build and adopt the BYOD approach in a more professional manner.

6.4 Risk Management

From our study, that there is clearly broad agreement on the importance of the availability of legislation and policies related to the use of BYOD, where approximately 75% of the questionnaire segment sees this importance, as shown in Fig 9. Additionally, our survey shows that respondents are concerned about security risks on personal devices or organisations' systems and data, which requires strict usage procedures [25, 39]. Many users believe in the importance of necessary legislation and strict procedures that led to a slight movement in this area represented in providing general frameworks for cybersecurity on their devices only. However, it is important to expand the scope of this framework to other relevant sectors, most importantly external users, to determine the criteria for users' acceptance to use the systems, summarised in the following:

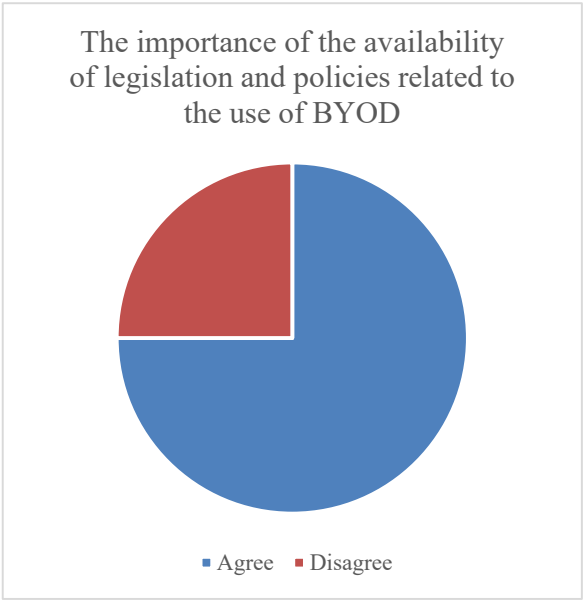


Fig 9: Importance of the availability of legislation and policies related to the use of BYOD

1. Define encrypted VPN communication channels.
2. Define various levels of user permissions distributed over all activities of users outside the organization.
3. Define password policies and their durations.
4. Define data policies and their level for availabilities and permissions.

In addition to these policies, there is a proposal for several policies related to the level of coding, networks, and operating systems, which represent another important part of this study and will be discussed in future studies.

Many potential risks that have been listed and detailed in the literature review on this topic show that they have not been addressed due to lack of awareness of organisations and institutions on the one hand, and working individuals on the other hand. Our study shows that the participants believe in the existence of high risks by 88.3%, as shown in Fig 10, but there is no institutional move in the many sectors whose members participated in our questionnaire. Therefore, one of the main factors in raising awareness of best practices is by educating individuals, which represents one of the important ways to increase chances of risk awareness at the individual and community levels, as well as clear legislation and policies.

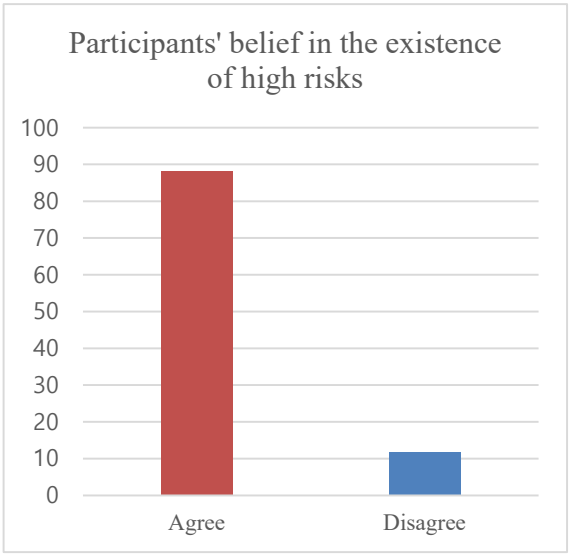


Fig 10: Participants' belief in the existence of high risks

Raising awareness mainly helps to reach acceptance and approval of this approach and thus the continuity of organisations and government agencies that view digital transformation as a future vision. Also, it provides the necessary remedies if any defect arises from breaching the policies of the BYOD approach. This is evidenced by our study that 79.04% of the participants believe in the importance of having regulatory and legislative policies to obtain the best benefits and reduce risks.

6.5 Perform Activity

In the era of COVID-19, e-services have increased rapidly, including several sectors such as healthcare and education. For example, in the first few weeks, the Ministry of Health in Saudi Arabia provided several platforms to provide the required services to support government efforts aimed at countering COVID-19. The Ministry of Education also provided several solutions to move towards the e-learning approach with the full lockdown, ensuring providing education to students during the pandemic. Providing required services to the citizens in the current period of COVID-19 leads organizations and government sectors in moving to digital transformation, which is the first step towards using BYOD.

Therefore, the Saudi government as represented in its 2030 vision and the National Transformation Program seeks to benefit from the current achievements of the technical ministries and their solutions during the pandemic, activating digital transformation for ministries, organisations, and other sectors by foreseeing the near and far future in digital transformation. Most sectors have included many rapid technological transformations within an integrated system of services that serve various segments of Saudi society. The sectors that have achieved rapid development mainly based on the BYOD approach are infrastructure of e-governments, health care, education, returnee travel platforms, supporting the private sector, e-commerce, working remotely in most governmental ministries, and providing new digital job opportunities to increase the motivation to return to normal life [42]. Additionally, many smartphone applications and technical platforms have been developed with advanced cloud technology for most ministries and government agencies to provide full support to end users. Therefore, the capabilities of SDAIA infrastructure effect integration and utilisation through a variety of ideas and future prospects and offering many features to increase digital transformation and continuous diffusion of the BYOD approach.

7. Implication

A variety of aspects emerge regarding the implications of using BYOD in governments and private sectors to increase technology adoption and automation for various processes in numerous sectors. The importance of taking advantage of the digital economy is clear, as well as having access to cloud data to implement various operations smoothly and competently with adequate privacy and security. Therefore, the importance of providing policies and standards consists mainly of delivery of fundamental frameworks for preserving required data and methods of business continuity. The National Cybersecurity Authority in Saudi Arabia has provided the infrastructure for these policies by obliging most government sectors to provide plans and policies for data preservation, methods of restoration, and business continuity, representing one of the main aspects of dealing with government sectors by using the BYOD approach to expansion in the future.

There is no doubt that the pandemic has given rise to many theoretical frameworks in practical forms, which are spread widely in various ways according to social requirements. Therefore, using BYOD in communities faces many challenges in implementation or reservations about its use, which shows the importance of using and sharing best practices among different communities to reach the best possible adoption. It could help to build theoretical frameworks that are tested in real environments in various sectors, companies, and organisations to offer useful methods that protect information and provide appropriate methods for its use.

Adding policies and standards could provide advance solutions at the security level for the device level. The security level in the devices requires strict policies that contain and document various risks and how to deal with them and look for the best solution to fill these gaps. Badly exploiting these gaps will contribute to weakening the infrastructure of government and companies sectors, resulting in the integration between systems or parties collapsing because of poorly written polices for data privacy, security, and integrity.

8. Conclusion

The BYOD trend is gaining popularity around the world. Its benefits are countless such as greater financial earnings, increased employee satisfaction, improved work efficiency, enhanced morale, and better flexibility. However, this trend also has its own challenges and risks while managing and controlling company data and networks. BYOD is vulnerable to viruses, malware, or spyware attacks that can access sensitive data, reveal information, modify access policies, disrupt services, create financial issues, reduce productivity, and result in legal implications. This research focuses on the status of the BYOD approach in health sector in Saudi Arabia based on the 5-step solution model through quantitative research methodology. The outcome of this research includes a statement of the users' knowledge of this trend, its prevalence, and their opinions of it with suggestion to increase the employee's awareness. Future work will investigate the general factors influencing the adoption of BYOD initiatives in government and private health sectors in Saudi Arabia, followed by specific factors that affect privacy and security in more detail, with proposed solutions addressing the output challenges.

Acknowledgments

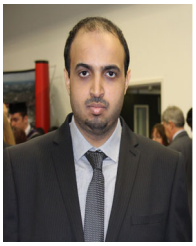
This research work was funded by the Makkah Digital Gate Initiative under Grant No. (MDP-IRI-13-2020). Therefore, authors gratefully acknowledge technical and financial support from the Emirate Of Makkah Province and King Abdulaziz University, Jeddah, Saudi Arabia.

References

[1] C. Matt, T. Hess, and A. Benlian, "Digital transformation strategies," Business & Information Systems Engineering, vol. 57, no. 5, pp. 339-343, 2015.
[2] 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.
[3] I. Mergel, N. Edelmann, and N. Haug, "Defining digital transformation: Results from expert interviews," Government Information Quarterly, vol. 36, no. 4, p. 101385, 2019.
[4] 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.
[5] Y. N. Azizaha et al., "Transformational or Transactional Leadership Style: Which Affects Work Satisfaction and Performance of Islamic University Lecturers During COVID-19 Pandemic," Systematic Reviews in Pharmacy, vol. 11, no. 7, pp. 577-588, 2020.
[6] S. C. o. Economic and D. Affairs, "Saudi vision 2030," 2016.
[7] A. S. Alharbi, G. Halikias, A. M. Basahel, and M. Yamin, "Digital Governments of Developed Nations and Saudi Arabia: A Comparative Study," in 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), 2020, pp. 255-260: IEEE.
[8] B. Carin, "G20 safeguards digital economy vulnerabilities with a financial sector focus," Economics: The Open-Access, Open-Assessment E-Journal, vol. 11, no. 2017-19, pp. 1-11, 2017.
[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] A. B. Garba, J. Armarego, D. Murray, and W. Kenworthy, "Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments," Journal of Information privacy and security, vol. 11, no. 1, pp. 38-54, 2015.
[11] 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.
[12] M. Finneran, "Mobile security gaps abound," Information Week, no. 1333, 2012.
[13] 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.
[14] N. Zahadat, P. Blessner, T. Blackburn, and B. A. Olson, "BYOD security engineering: A framework and its analysis," Computers & Security, vol. 55, pp. 81-99, 2015.
[15] M. P. Morolong, F. B. Shava, and A. M. Gamundani, "Bring Your Own Device (BYOD) Information Security Risks: Case of Lesotho," in International Conference on Cyber Warfare and Security, 2020, pp. 346-XVI: Academic Conferences International Limited.
[16] 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.
[17] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and privacy considerations," It Professional, vol. 14, no. 5, pp. 53-55, 2012.
[18] 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.
[19] K. E. Welsh, A. L. Mauchline, D. France, V. Powell, W. B. Whalley, and J. Park, "Would Bring Your Own Device (BYOD) be welcomed by undergraduate students to support their learning during fieldwork?," Journal of Geography in Higher Education, vol. 42, no. 3, pp. 356-371, 2018.
[20] A. V. Herrera, M. Ron, and C. Rabadão, "National cyber-security policies oriented to BYOD (bring your own device): Systematic review," in 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), 2017, pp. 1-4: IEEE.
[21] F. Portela, A. M. da Veiga, and M. F. Santos, "Benefits of bring your own device in healthcare," in Next-Generation Mobile and Pervasive Healthcare Solutions: IGI Global, 2018, pp. 32-45.
[22] 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.
[23] M. Shabazi, M. Amini Rarani, S. Tahmasebian, and M. Jahanbakhsh, "BYOD and its Application in the Healthcare Environment," Applied Health Information Technology, vol. 1, no. 1, pp. 60-64, 2020.
[24] M. H. U. Sharif, R. Datta, S. N. Sankarasetty, H. Garikapati, M. Valavala, and S. Maraboyina, "BRING YOUR OWN DEVICE (BYOD) PROGRAM," International Journal of Engineering Applied Sciences and Technology, vol. 4, no. 4, pp. 2455-2143, 2019.
[25] 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.
[26] 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.
[27] 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.
[28] B. Morrow, "BYOD security challenges: control and protect your most sensitive data," Network Security, vol. 2012, no. 12, pp. 5-8, 2012.
[29] M. Dhingra, "Legal issues in secure implementation of bring your own device (BYOD)," Procedia Computer Science, vol. 78, pp. 179-184, 2016.
[30] 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.
[31] 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.
[32] B. Lebek, K. Degirmenci, and M. Breitner, "Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices," in Proceedings of the nineteenth Americas conference on information systems, 2013, pp. 1-8: Association for Information Systems (AIS).
[33] A. Gustav and S. Kabanda, "BYOD adoption concerns in the South African financial institution sector," in CONF-IRM, 2016, p. 59.
[34] J. E. Moyer, "Managing mobile devices in hospitals: A literature review of BYOD policies and usage," Journal of Hospital Librarianship, vol. 13, no. 3, pp. 197-208, 2013.
[35] K. AlHarthy and W. Shawkat, "Implement network security control solutions in BYOD environment," in 2013 IEEE International Conference on Control System, Computing and Engineering, 2013, pp. 7-11: IEEE.
[36] A. Scarfo, "New security perspectives around BYOD," in 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, 2012, pp. 446-451: IEEE.
[37] 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.
[38] M. F. Mohammed, "Privacy and Social Networking: WhatsApp Users' Perception in Saudi Arabia Researchers: Ms. Nemah Alsayed Ms. Haifaa Alakel," 2016.
[39] P. Saa, O. Moscoso-Zea, and S. Lujan-Mora, "Bring your own device (BYOD): Students perception—Privacy issues: A new trend in education?," in 2017 16th International Conference on Information Technology Based Higher Education and Training (ITHET), 2017, pp. 1-5: IEEE.
[40] F. Mohammed, F. Olayah, A. Ali, and N. A. Gazem, "The effect of cloud computing adoption on the sustainability of e-government services: A review," International Journal of Advanced Science and Technology, vol. 29, no. 5, pp. 2636-2642, 2020.
[41] https://www.imf.org/ar/News/Articles/2020/11/06/blog-bridging-digital-divide-to-scale-up-covid19-recovery
[42] https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2020/RDF/Presentations/Session1/KSA.pdf
[43] Michelberger, Pál, and Pál Fehér-Polgár. "BYOD SECURITY STRATEGY (ASPECTS OF A MANAGERIAL DECISION)." Journal of Security & Sustainability Issues 9.4 (2020).

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.



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.